Capacity Results for Relay Channels with Confidential Messages

Yasutada Oohama and Shun Watanabe

***Abstract*— We consider a communication system where a relay helps transmission of messages from a sender to a receiver. The relay is considered not only as a helper but as a wire-tapper who can obtain some knowledge about transmitted messages. In this paper we study a relay channel with confidential messages(RCC), where a sender attempts to transmit common information to both a receiver and a relay and also has private information intended for the receiver and confidential to the relay. The level of secrecy of private information confidential to the relay is measured by the equivocation rate, i.e., the entropy rate of private information conditioned on channel outputs at the relay. The performance measure of interest for the RCC is the rate triple that includes the common rate, the private rate, and the equivocation rate as components. The rate-equivocation region is defined by the set that consists of all these achievable rate triples. In this paper we give two definitions of the rate-equivocation region. We first define the rate-equivocation region in the case of deterministic encoder and call it the deterministic rate-equivocation region. Next, we define the rate-equivocation region in the case of stochastic encoder and call it the stochastic rate-equivocation region. We derive explicit inner and outer bounds for the above two rate-equivocation regions. On the deterministic/stochastic rate-equivocation region we present two classes of relay channels where inner and outer bounds match. We also evaluate the deterministic and stochastic rate-equivocation regions of the Gaussian RCC.**

***Index Terms*— Relay channel, confidential messages, information security**

I. Introduction

Security of communications can be studied from information theoretical viewpoint by regarding them as a communication system in which some messages transmitted through channel should be confidential to anyone except for authorized receivers.

Information theoretical approach to security problem in communications was first attempted by Shannon [1]. He discussed a theoretical model of cryptosystems using the framework of classical one way noiseless channels and derived some conditions for secure communication. Yamamoto [2],[3] investigated some extensions of Shannon's cipher system.

Various types of multi-terminal communication systems have been investigated so far in the field of multi-user information theory. In those systems we can consider the case where a confidentiality of transmitted messages is required from standpoint of security. In this case it is of importance to analyze security of communications from viewpoint of multi-user information theory.

Y. Oohama and S. Watanabe are with the Department of Information Science and Intelligent Systems, University of Tokushima, 2-1 Minami Josanjima-Cho, Tokushima 770-8506, Japan.

The security of communication for the broadcast channel was studied by Wyner [4] and Csiszár and Körner [5]. Yamamoto [6]-[10] studied several secure communication systems under the framework of multi-terminal source or channel coding systems. Maurer [11], Ahlswede and Csiszár [12], Csiszár and Narayan [13]-[15], studied public key agreements under the framework of multi-user information theory. Oohama [16] discussed the security of communication for the relay channel. He posed and investigated the relay channel with confidential messages, where the relay acts as both a helper and a wire-tapper. Subsequently, the above security problem in relay communication was studied in detail by Oohama [17] and He and Yener [18], [19]. Liang and Poor [20] discussed the security of communication for the multiple access channel. They formulated and studied the multiple access channel with confidential messages. Liu et al. [21] considered interference and broadcast channels with confidential messages. Tekin and Yener [22] studied general Gaussian multiple access and two way wire tap channels. Lai and El Gamal [23] investigated the security of relay channels in a problem set up different form [16].

In this paper we discuss the security of communication for the relay channel under the framework that Oohama introduced in [16]. In the relay channel a relay is considered not only as a sender who helps transmission of messages but as a wire-tapper who wish to know something about the transmitted messages. Coding theorem for the relay channel was first established by Cover and El Gamal [24]. By carefully checking their coding scheme used for the proof of the direct coding theorem, we can see that in their scheme the relay helps transmission of messages by learning all of them. Hence, this coding scheme is not adequate when some messages should be confidential to the relay.

Oohama [16] studied the security of communication for the relay channel under the situation that some of transmitted messages should be confidential to the relay. For analysis of this situation Oohama posed the communication system called the relay channel with confidential messages or briefly said the RCC. In the RCC, a sender wishes to transmit two types of messages. One is a message called *a common message* which is sent to a legitimate receiver and a relay. The other is a message called *a private message* which is sent only to the legitimate receiver and should be confidential to the relay as much as possible. The level of secrecy of private information confidential to the relay can be measured by the equivocation rate, i.e., the entropy rate of private messages conditioned on channel outputs at the relay. The performance measure of interest is the rate triple that includes the transmission rates of common and private messages and the equivocation

rate as components. We refer to the set that consists of all achievable rate triples as the rate-equivocation region. Oohama [16] derived an inner bound of the rate-equivocation region.

In this paper we study the coding problem of the RCC. In general two cases of encoding can be considered in the problem of channel coding. One is a case where deterministic encoders are used for transmission of messages and the other is a case where stochastic encoders are used. It is well known that for problems involving secrecy, randomization of encoding enhances the security of communication. From this reason, stochastic encoding was always assumed in the previous works treating security problems in communication. However, in those works it is not clear how much advantage stochastic encoding can offer in secure communication. To know a merit of stochastic encoding precisely we must also know a fundamental theoretical limit of secure communication when encoding is restricted to be *deterministic*. In this paper we discuss security problems in the RCC in two cases. One is a case of deterministic encoder, where the sender must use a deterministic encoder. The other is a case of stochastic encoder, where the sender is allowed to use a stochastic encoder. The former case models an *insecure* communication scheme and the latter case models a *secure* communication scheme. We define two rate-equivocation regions. One is a rate-equivocation region in the case of deterministic encoder and call it the deterministic rate-equivocation region. The other is a rate-equivocation region in the case of stochastic encoder and call it the stochastic rate-equivocation region.

In this paper, we derive several results on the deterministic and stochastic rate-equivocation regions. [1] Cover and El Gamal [24] determined the capacity for two classes of relay channels. One is a degraded relay channel and the other is a reversely degraded channel. In the degraded relay channel, channel outputs obtained by the relay are less noisy than those obtained by the receiver. Conversely, in the reversely degraded relay channel, channel outputs obtained by the relay are more noisy than those obtained by the receiver. Our capacity results have a close connection with the above two classes of relay channels.

On the deterministic rate-equivocation region, we derive two pairs of inner and outer bounds. On the first pair of inner and outer bounds we show that they match for the class of reversely degraded relay channels. Furthermore, we show that if the relay channel is degraded, no security is guaranteed for transmission of private messages. On the second pair of inner and outer bounds we show that they match for the class of relay channels having some deterministic component in their stochastic matrix. We further derive an explicit outer bound effective for a class of relay channels where channel outputs obtained by the relay depend only on channel inputs from the sender.

On the stochastic rate-equivocation region, we derive two pairs of inner and outer bounds. On the first pair, inner and outer bound match for the class of reversely degraded channels. On the second one, inner and outer bounds match for the class of semi deterministic relay channels. We show that when the relay channel is degraded, no security is guaranteed for transmission of private messages even if we use stochastic encoders.

We compare the deterministic rate-equivocation region with the stochastic rate-equivocation region to show that the former is strictly smaller than the latter. It is obvious that the maximum secrecy rate attained by the deterministic encoding does not exceed that of stochastic encoding. We demonstrate that for the reversely degraded relay channel the former is equal to the latter.

When the relay is kept completely ignorant of private message in the RCC, we say that the prefect secrecy is established. We show that the prefect secrecy can hardly be attained by the deterministic encoder. In the case of stochastic encoder the secrecy capacity is defined by the maximum transmission rate of private message under the condition of prefect secrecy. From the results on the stochastic rate-equivocation regions, we can obtain inner and outer bounds of the stochastic secrecy capacities. In particular, when the relay channel is reversely degraded or semi deterministic, we determine the stochastic secrecy capacity.

We also study the Gaussian RCC, where transmissions are corrupted by additive Gaussian noise. We evaluate the deterministic and stochastic rate-equivocation regions of the Gaussian RCC. For each rate-equivocation we derive a pair of explicit inner and outer bounds to show that those bounds match for the class of reversely degraded relay channels.

On our results on the inner bounds of the rate-equivocation region we give their rigorous proofs. The method Csiszár and Körner [5] used for computation of the equivocation is a combinatorial method based on the type of sequences [25]. Their method has a problem that it is not directly applicable to the Gaussian case. To overcome this problem we introduce a new unified way of estimating error probabilities and equivocation rate for both discrete and Gaussian cases. Our method is based on the information spectrum method introduced and developed by Han [26]. Our derivation of the inner bounds is simple and straightforward without using any particular property on the sets of jointly typical sequences.

In the RCC, the relay also act as a receiver with respect to the common message. This implies that when there is no security requirement in the RCC, its communication scheme is equal to that of a special case of cooperative relay broadcast channels(RBCs) posed and investigated by Liang and Veeravalli [27] and Liang and Kramer [28]. Cooperation and security are two important features in communication networks. Coding problems for the RCC provide an interesting interplay between cooperation and security.

II. Relay Channels with Confidential Messages

Let $\mathcal{X}, \mathcal{S}, \mathcal{Y}, \mathcal{Z}$ be finite sets. The relay channel dealt with in this paper is defined by a discrete memoryless channel specified with the following stochastic matrix:

$$\Gamma \stackrel{\triangle}{=} \{\Gamma(y,z \mid x,s)\}_{(x,s,y,z)\in\mathcal{X}\times\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}. \tag{1}$$

Let X be a random variable taking values in $\mathcal{X}$ and $X^n = X_1X_2\cdots X_n$ be a random vector taking values in $\mathcal{X}^n$. We

[1] The same determination problems of the two rate-equivocation regions were investigated by Oohama [17]. However, his results on the deterministic rate-equivocation region contain some mistakes. The results on the deterministic rate-equivocation we derive in this paper correct those mistakes.

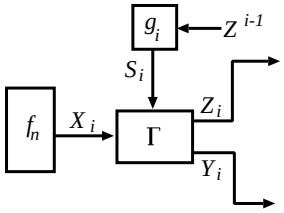

Fig. 1. Channel inputs and outputs at the ith transmission.

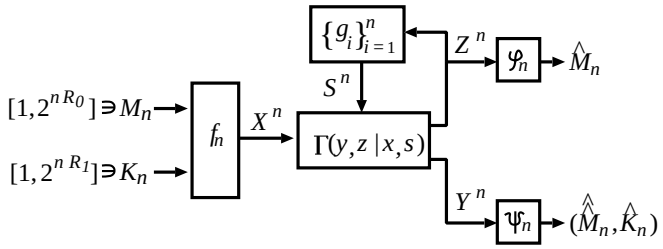

Fig. 2. Transmission of messages via relay channel using $(f_n, \{g_i\}_{i=1}^n, \psi_n, \varphi_n)$.

write an element of $\mathcal{X}^n$ as $\boldsymbol{x} = x_1 x_2 \cdots x_n$. Similar notations are adopted for S, Y, and Z.

In the RCC, we consider the following scenario of communication. Let K_n and M_n be uniformly distributed random variables taking values in message sets $\mathcal{K}_n$ and $\mathcal{M}_n$, respectively. The random variable M_n is a common message sent to a relay and a legitimate receiver. The random variable K_n is a private message sent only to the receiver and contains an information confidential to the relay. A sender transforms K_n and M_n into a transmitted sequence X^n using an encoder function f_n and sends it to the relay and the legitimate receiver. For the encoder function f_n, we consider two cases; one is the case where f_n is *deterministic* and the other is the case where f_n is *stochastic*. In the former case f_n is a one to one mapping from $\mathcal{K}_n \times \mathcal{M}_n$ to $\mathcal{X}^n$. In the latter case $f_n : \mathcal{K}_n \times \mathcal{M}_n \to \mathcal{X}^n$ is a stochastic matrix defined by

$$f_n(k,m) = \{f_n(\boldsymbol{x}|k,m)\}_{\boldsymbol{x}\in\mathcal{X}^n}, (k,m) \in \mathcal{K}_n \times \mathcal{M}_n\,.$$

Here, $f_n(\boldsymbol{x}|k,m)$ is a probability that the encoder f_n generates a channel input $\boldsymbol{x}$ from the message pair (k,m). Channel inputs and outputs at the ith transmission is shown in Fig. 1. At the ith transmission, the relay observes the random sequence $Z^{i-1} \triangleq (Z_1, Z_2, \cdots, Z_{i-1})$ transmitted by the sender through noisy channel, encodes them into the random variable S_i and sends it to the receiver.

The relay also wishes to decode the common message from observed channel outputs. The encoder function at the relay is defined by the sequence of functions $\{g_i\}_{i=1}^n$. Each g_i is defined by $g_i : \mathcal{Z}^{i-1} \to \mathcal{S}$. Note that the channel input S_i that the relay sends at the ith transmission depends solely on the output random sequence Z^{i-1} that the relay previously obtained as channel outputs. The decoding functions at the legitimate receiver and the relay are denoted by ψ_n and φ_n, respectively. Those functions are formally defined by $\psi_n : \mathcal{Y}^n \to \mathcal{K}_n \times \mathcal{M}_n\,, \varphi_n : \mathcal{Z}^n \to \mathcal{M}_n$. Transmission of messages via relay channel using $(f_n, \{g_i\}_{i=1}^n, \psi_n, \varphi_n)$ is shown in Fig. 2. When f_n is a deterministic encoder, the joint probability mass function on $\mathcal{K}_n \times \mathcal{M}_n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned}&\Pr\{(K_n, M_n, Y^n, Z^n) = (k, m, \boldsymbol{y}, \boldsymbol{z})\}\\ &= \frac{1}{|\mathcal{K}_n||\mathcal{M}_n|}\prod_{i=1}^n \Gamma\big(y_i, z_i\,\big|x_i(k,m), g_i(z^{i-1})\big)\,,\end{aligned}$$

where $x_i(k,m)$ is the ith component of $\boldsymbol{x} = f_n(k,m)$ and $|\mathcal{K}_n|$ is a cardinality of the set $\mathcal{K}_n$. When f_n is a stochastic encoder, the joint probability mass function on $\mathcal{K}_n \times \mathcal{M}_n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned}&\Pr\{(K_n, M_n, X^n, Y^n, Z^n) = (k, m, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})\}\\ &= \frac{f_n(\boldsymbol{x}|k,m)}{|\mathcal{K}_n||\mathcal{M}_n|}\prod_{i=1}^n \Gamma\big(y_i, z_i\,\big|x_i(k,m), g_i(z^{i-1})\big)\,.\end{aligned}$$

Error probabilities of decoding at the receiver and the relay are defined by

$$\begin{aligned}\lambda_1^{(n)} &\triangleq \Pr\{\psi_n(Y^n) \neq (K_n, M_n)\} \text{ and}\\ \lambda_2^{(n)} &\triangleq \Pr\{\varphi_n(Z^n) \neq M_n\},\end{aligned}$$

respectively.

In the RCC, the relay act as a *wire-tapper* with respect to the private message K_n. The level of ignorance of the relay with respect to K_n is measured by the equivocation rate, i.e., the entropy rate $\frac{1}{n}H(K_n|Z^n)$ conditioned on the channel output Z^n at the relay. Throughout the paper, the logarithmic function is to the base 2. The equivocation rate should be greater than or equal to a prescribed positive level.

A triple $(R_0, R_1, R_{\rm e})$ is *achievable* if there exists a sequence of quadruples $\{(f_n, \{g_i\}_{i=1}^n, \psi_n, \varphi_n)\}_{n=1}^\infty$ such that

$$\begin{aligned}&\lim_{n\to\infty}\lambda_1^{(n)} = \lim_{n\to\infty}\lambda_2^{(n)} = 0,\\ &\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{M}_n| = R_0,\ \lim_{n\to\infty}\ \frac{1}{n}\log|\mathcal{K}_n| = R_1,\\ &\lim_{n\to\infty}\frac{1}{n}H(K_n|Z^n) \geq R_{\rm e}\,.\end{aligned}$$

When f_n and $\{g_i\}_{n=1}$ are restricted to be deterministic, the set that consists of all achievable rate triple is denoted by $\mathcal{R}_{\rm d}(\Gamma)$, which is called the deterministic rate-equivocation region of the RCC. When f_n is allowed to be stochastic and $\{g_i\}_{n=1}$ is restricted to be deterministic, the set that consists of all achievable rate triple is denoted by $\mathcal{R}_{\rm s}(\Gamma)$, which is called the stochastic rate-equivocation region. Main results on $\mathcal{R}_{\rm d}(\Gamma)$ and $\mathcal{R}_{\rm s}(\Gamma)$ will be described in the next section.

In the above problem set up the relay encoder $\{g_i\}_{i=1}^n$ is a *deterministic encoder*. We can also consider the case where we may use a *stochastic encoder* as $\{g_i\}_{i=1}^n$. In this case the relay function $g_i(z^{i-1}) \in \mathcal{S}$, $z^{i-1} \in \mathcal{Z}^{i-1}$ is a stochastic matrix given by

$$g_i(z^{i-1}) = \big\{g_i(s|z^{i-1})\big\}_{s\in\mathcal{S}}\,.$$

Here $g_i(s|z^{i-1})$ is a conditional probability of $S_i = s$ conditioned on $Z^{i-1} = z^{i-1}$. When f_n is deterministic and $\{g_i\}_{i=1}^n$ is stochastic, the joint probability mass function on $\mathcal{K}_n \times \mathcal{M}_n \times \mathcal{S}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned}&\Pr\{(K_n, M_n, S^n, X^n, Y^n, Z^n) = (k, m, \boldsymbol{s}, \boldsymbol{y}, \boldsymbol{z})\}\\ &= \frac{1}{|\mathcal{K}_n||\mathcal{M}_n|}\prod_{i=1}^n \Gamma(y_i, z_i\,|x_i(k,m), s_i)\,g_i(s_i|z^{i-1}).\end{aligned}$$

When f_n and $\{g_i\}_{i=1}^n$ are stochastic, the joint probability mass function on $\mathcal{K}_n \times \mathcal{M}_n \times \mathcal{S}^n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$ is given by

$$\begin{aligned}&\Pr\{(K_n, M_n, S^n, X^n, Y^n, Z^n) = (k, m, \boldsymbol{s}, \boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})\}\\ &= \frac{f_n(\boldsymbol{x}|k,m)}{|\mathcal{K}_n||\mathcal{M}_n|}\prod_{i=1}^n \Gamma(y_i, z_i\,|x_i(k,m), s_i)\, g_i(s_i|z^{i-1}).\end{aligned}$$

Capacity results in the case of stochastic relay encoder will be stated in Section III-C.

In the remaining part of this section, we state relations between the RCC and previous works. When $|\mathcal{S}| = 1$, Γ becomes a broadcast channel, and the coding scheme of the RCC coincides with that of the broadcast channel with confidential messages(the BCC) investigated by Csiszár and Körner [5]. They determined the stochastic rate-equivocation region for the BCC.

Liang and Veeravalli [27] and Liang and Krammer [28] posed and investigated a new theoretical model of cooperative communication network called the partially/fully cooperative relay broadcast channel(RBC). The RCC can be regarded as a communication system where a security requirement is imposed on the RBC. In fact, setting

$$\mathcal{C}_{\rm rbc}(\Gamma) \stackrel{\triangle}{=} \mathcal{R}_{\rm d}(\Gamma) \cap \{(R_0, R_1, R_{\rm e}) : R_{\rm e} = 0\},$$

$\mathcal{C}_{\rm rbc}(\Gamma)$ defines the capacity region of a special case of the partially cooperative RBC. Liang and Veeravalli [27] and Liang and Krammer [28] considered the determination problem of $\mathcal{C}_{\rm rbc}(\Gamma)$ and determined it for some class of relay channels. The determination problem of $\mathcal{C}_{\rm rbc}(\Gamma)$ for general Γ still remains open.

III. Main Results

In this section we state our main results. Proofs of the results are stated in Sections VI and VII.

A. Deterministic Coding Case

In this subsection we state our results on inner and outer bounds of $\mathcal{R}_{\rm d}(\Gamma)$. Let U be an auxiliary random variable taking values in finite set $\mathcal{U}$. Define the set of random triples $(U,\, X,\, S) \in \mathcal{U} \times \mathcal{X} \times \mathcal{S}$ by

$$\begin{aligned}\mathcal{P}_1 \stackrel{\triangle}{=} \{(U,X,S) :\ &|\mathcal{U}| \le |\mathcal{X}||\mathcal{S}| + 3\,,\\ &U \to XS \to YZ\}\,,\end{aligned}$$

where $U \to XS \to YZ$ means that random variables $U, (X,S)$ and (Y,Z) form a Markov chain in this order. Set

$$\begin{aligned}\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_0,R_1,R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,,\\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,,\\ &R_1 \le I(X;Y|US)\,,\\ &R_{\rm e} \le [R_1 - I(X;Z|US)]^+ .\}\,,\\ \tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_0,R_1,R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,,\\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,,\\ &R_1 \le I(X;YZ|US)\,,\\ &R_0 + R_1 \le I(XS;Y)\,,\\ &R_{\rm e} \le [R_1 - I(X;Z|US)]^+ .\}\,,\end{aligned}$$

where $[a]^+ = \max\{0, a\}$. Set

$$\begin{aligned}\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(U,X,S|\Gamma)\,,\\ \tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(U,X,S|\Gamma)\,.\end{aligned}$$

Then we have the following.

Theorem 1: For any relay channel Γ,

$$\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma) \subseteq \tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)\,.$$

An essential difference between $\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma)$ and $\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$ is a gap Δ given by

$$\begin{aligned}\Delta &\stackrel{\triangle}{=} I(X;Y|ZUS) - [I(X;Y|US) - I(X;Z|US)]\\ &= I(X;ZY|US) - I(X;Y|US) = I(X;Z|YUS)\,.\end{aligned}$$

Observe that

$$\begin{aligned}\Delta &= H(Z|YUS) - H(Z|YXUS)\\ &\stackrel{\rm (a)}{=} H(Z|YUS) - H(Z|YXS)\\ &\le H(Z|YS) - H(Z|YXS) = I(X;Z|YS)\,.\end{aligned}$$

Equality (a) follows from the Markov condition $U \to XS \to YZ$. Hence, Δ vanishes if the relay channel $\Gamma = \{\Gamma(z,y|x,s)\}_{(x,s,y,z)\in\mathcal{X}\times\mathcal{S}\times\mathcal{Y}\times\mathcal{Z}}$ satisfies the following:

$$\Gamma(z,y|x,s) = \Gamma(z|y,s)\Gamma(y|x,s). \tag{2}$$

The above condition is equivalent to the condition that X, S, Y, Z form a Markov chain $X \to SY \to Z$ in this order. Cover and El. Gamal [24] called this relay channel the reversely degraded relay channel. On the other hand, we have

$$\begin{aligned}&I(X;Y|ZUS) = H(Y|ZUS) - H(Y|ZXUS)\\ &\le H(Y|ZS) - H(Y|ZXS) = I(X;Y|ZS)\,,\end{aligned} \tag{3}$$

where the last inequality follows from the Markov condition $U \to XSZ \to Y$. From (3) we can see that the quantity $I(X;Y|ZUS)$ vanishes if the relay channel Γ satisfies the following:

$$\Gamma(z,y|x,s) = \Gamma(y|z,s)\Gamma(z|x,s). \tag{4}$$

Hence, if the relay channel Γ satisfies (4), then, $R_{\rm e}$ should be zero. This implies that no security on the private messages is guaranteed. The condition (4) is equivalent to the condition that X, S, Y, Z form a Markov chain $X \to SZ \to Y$ in this order. Cover and El. Gamal [24] called this relay channel the degraded relay channel. Summarizing the above arguments, we obtain the following two corollaries.

Corollary 1: For the reversely degraded relay channel Γ,

$$\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) = \mathcal{R}_{\rm d}(\Gamma) = \tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)\,.$$

Corollary 2: In the deterministic coding case, if the relay channel Γ is degraded, then no security on the private messages is guaranteed.

Corollary 1 implies that the suggested strategy in Theorem 1 is optimal in the case of reversely degraded relay channels. Corollary 2 meets our intuition in the sense that if the relay channel is degraded, the relay can do anything that the destination can.

Next we define another pair of inner and outer bounds. Define a set of random triples $(U,X,\ S) \in \mathcal{U} \times \mathcal{X} \times \mathcal{S}$ by

$$\mathcal{P}_2 \stackrel{\triangle}{=} \{(U,X,S):\ |\mathcal{U}| \le |\mathcal{Z}||\mathcal{X}||\mathcal{S}|+3\,, \\ U \to XSZ \to Y\}\,.$$

It is obvious that $\mathcal{P}_1 \subseteq \mathcal{P}_2$. Set

$$\begin{aligned}
&\mathcal{R}_{\rm d}^{(\rm in)}(U,X,S|\Gamma) \\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}) : R_0,R_1,R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\
&\quad R_0+R_1 \le I(X;Y|US) \\
&\qquad\quad + \min\{I(U;Z|S), I(US;Y)\}\,, \\
&\quad R_{\rm e} \le [R_1 - I(X;Z|US)]^+\,, \\
&\quad R_{\rm e} \le [I(X;Y|US) - I(X;Z|US)]^+ .\}\,, \\
&\mathcal{R}_{\rm d}^{(\rm out)}(U,X,S|\Gamma) \\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}) : R_0,R_1,R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\
&\quad R_0+R_1 \le I(X;Y|US) \\
&\qquad\quad + \min\{I(U;Z|S), I(US;Y)\}\,, \\
&\quad R_{\rm e} \le [R_1 - I(X;Z|US) + I(U;Z|XS)]^+\,, \\
&\quad R_{\rm e} \le [I(X;Y|US) - I(X;Z|US)]^+ .\}\,.
\end{aligned}$$

Furthermore, set

$$\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) \stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \mathcal{R}_{\rm d}^{(\rm in)}(U,X,S|\Gamma)\,,$$

$$\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma) \stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_2} \mathcal{R}_{\rm d}^{(\rm out)}(U,X,S|\Gamma)\,.$$

Then, we have the following theorem.

Theorem 2: For any relay channel Γ,

$$\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma) \subseteq \mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)\,.$$

Here we consider a class of relay channels in which Z is a function of XS. We call this class of relay channels the semi deterministic relay channel. If Γ is semi deterministic, $U \to XS \to Z$ for any $(U,X,S) \in \mathcal{P}_2$. On the other hand, we have $U \to ZXS \to Y$ for any $(U,X,S) \in \mathcal{P}_2$. From those two Markov chains we have $U \to XS \to YZ$, which implies that $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) = \mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$. Summarizing the above argument we have the following.

Corollary 3: If Γ belongs to the class of semi deterministic relay channels,

$$\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma) = \mathcal{R}_{\rm d}(\Gamma) = \mathcal{R}_{\rm d}^{(\rm in)}(\Gamma)\,.$$

Finally, we derive the third outer bound of $\mathcal{R}_{\rm d}(\Gamma)$ which is effective for a certain class of relay channels. We consider the case where the relay channel Γ satisfies

$$\Gamma(y,z|x,s) = \Gamma(y|z,x,s)\Gamma(z|x). \tag{5}$$

The above condition on Γ is equivalent to the condition that X,S,Z satisfy the Markov chain $S \to X \to Z$. This condition corresponds to a situation where the outputs of the relay encoder does not directly affect the communication from the sender to the relay. This situation can be regarded as a natural communication link in practical relay communication systems. In this sense we say that the relay channel Γ belongs to the class of natural communication link or briefly the class NL if it satisfies (5).

For given $(U,X,S) \in \mathcal{U} \times \mathcal{X} \times \mathcal{S}$, set

$$\begin{aligned}
&\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(U,X,S|\Gamma) \\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}) : R_0,R_1,R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \min\{I(U;Y), I(U;Z|S)\}\,, \\
&\quad R_0+R_1 \le I(X;Y|US) \\
&\qquad\quad + \min\{I(US;Y), I(U;Z|S)+\zeta(S;Y,Z|U)\}\,, \\
&\quad R_{\rm e} \le [R_1 - I(X;Z|US)]^+\,, \\
&\quad R_{\rm e} \le [I(X;Y|US) - I(X;Z|US) + \zeta(S;Y,Z|U)]^+ .\}\,,
\end{aligned}$$

where we set

$$\begin{aligned}
\zeta(S;Y,Z|U) &\stackrel{\triangle}{=} I(XS;Y|U) - I(XS;Z|U) \\
&\quad -[I(X;Y|US) - I(X;Z|US)] \\
&= I(S;Y|U) - I(S;Z|U) \\
&= H(S|ZU) - H(S|YU)\,.
\end{aligned}$$

The quantity $\zeta(S;Y,Z|U)$ satisfies the following.

Property 1: For any $(U,X,S) \in \mathcal{P}_2$,

$$\zeta(S;Y,Z|U) \le \min\{H(S|Z), I(XS;Y|Z)\}\,.$$

Proof: It is obvious that $\zeta(S;Y,Z|U) \le H(S|Z)$. We prove $\zeta(S;Y,Z|U) \le I(XS;Y|Z)$. We have the following chain of inequalities:

$$\begin{aligned}
&\zeta(S;Y,Z|U) = H(S|ZU) - H(S|YU) \\
&\le H(S|ZU) - H(S|YZU) = I(S;Y|ZU) \\
&= H(Y|ZU) - H(Y|ZUS) \\
&\le H(Y|Z) - H(Y|ZUS) \\
&\le H(Y|Z) - H(Y|ZXSU) \\
&= H(Y|Z) - H(Y|ZXS) = I(XS;Y|Z),
\end{aligned}$$

where the last equality follows from the Markov condition $U \to ZXS \to Y$. ■

Set

$$\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma) \stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \hat{\mathcal{R}}_{\rm d}^{(\rm out)}(U,X,S|\Gamma)\,.$$

Our result is the following.

Theorem 3: If Γ belongs to the class NL, we have

$$\mathcal{R}_{\rm d}(\Gamma) \subseteq \hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)\,.$$

It is obvious that if $\zeta(S;Y,Z|U) \le 0$ for $(U,X,S) \in \mathcal{P}_1$, we have

$$\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) = \mathcal{R}_{\rm d}(\Gamma) = \hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma).$$

By Property 1, the condition that

$$\min\{H(S|Z), I(XS,Y|Z)\} = 0 \text{ for any } (X,S) \tag{6}$$

is a sufficient condition for $\zeta(S;Y,Z|U)$ to be non positive on $(U,X,S) \in \mathcal{P}_1$. The condition (6) on Γ is very severe. We do not have found so for any effective condition on Γ such that $\zeta(S;Y,Z|U) \le 0$ for any $(U,X,S) \in \mathcal{P}_1$. When $|\mathcal{S}| = 1$, then by Property 1, we have $\zeta(S;Y,Z|U) \le 0$. Hence $\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$ coincides with $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma)$. In this case, the class NL becomes a class of general broadcast channels with

one output and two input. Thus, the coding strategy achieving $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma)$ in Theorem 2 is optimal in the case of BCC and deterministic coding.

B. Stochastic Encoding Case

In this subsection we state our results on inner and outer bounds of $\mathcal{R}_{\rm s}(\Gamma)$. Set

$$\begin{aligned}
&\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(U,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}): 0\le R_0, 0\le R_{\rm e}\le R_1,\\
&\quad R_0\le \min\{I(US;Y), I(U;Z|S)\},\\
&\quad R_1\le I(X;Y|US),\\
&\quad R_{\rm e}\le [I(X;Y|US)-I(X;Z|US)]^+\},\\
&\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(U,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}): 0\le R_0, 0\le R_{\rm e}\le R_1,\\
&\quad R_0\le \min\{I(US;Y), I(U;Z|S)\},\\
&\quad R_1\le I(X;YZ|US),\\
&\quad R_0+R_1\le I(XS;Y),\\
&\quad R_{\rm e}\le I(X;Y|ZUS).\}.
\end{aligned}$$

Furthermore, set

$$\begin{aligned}
\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(U,X,S|\Gamma),\\
\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(U,X,S|\Gamma).
\end{aligned}$$

We further present another pair of inner and outer bounds of $\mathcal{R}_{\rm s}(\Gamma)$. To this end define sets of random quadruples $(U,V,X,S) \in \mathcal{U}\times\mathcal{V}\times\mathcal{X}\times\mathcal{S}$ by

$$\begin{aligned}
\mathcal{Q}_1 &\stackrel{\triangle}{=} \{(U,V,X,S): |\mathcal{U}|\le|\mathcal{X}||\mathcal{S}|+3,\\
&\qquad |\mathcal{V}|\le(|\mathcal{X}||\mathcal{S}|)^2+4|\mathcal{X}||\mathcal{S}|+3,\\
&\qquad U\to V\to XS\to YZ, US\to V\to X.\},\\
\mathcal{Q}_2 &\stackrel{\triangle}{=} \{(U,V,X,S): |\mathcal{U}|\le|\mathcal{Z}||\mathcal{X}||\mathcal{S}|+3,\\
&\qquad |\mathcal{V}|\le(|\mathcal{Z}||\mathcal{X}||\mathcal{S}|)^2+4|\mathcal{Z}||\mathcal{X}||\mathcal{S}|+3,\\
&\qquad U\to V\to XSZ\to Y, US\to VX\to Z,\\
&\qquad US\to V\to X.\}.
\end{aligned}$$

It is obvious that $\mathcal{Q}_1\subseteq\mathcal{Q}_2$. For given $(U,V,X,S)\in\mathcal{U}\times\mathcal{V}\times\mathcal{X}\times\mathcal{S}$, set

$$\begin{aligned}
&\mathcal{R}(U,V,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \{(R_0,R_1,R_{\rm e}): 0\le R_0, 0\le R_{\rm e}\le R_1,\\
&\quad R_0\le\min\{I(US;Y), I(U;Z|S)\},\\
&\quad R_0+R_1\le I(V;Y|US)+\min\{I(US;Y), I(U;Z|S)\},\\
&\quad R_{\rm e}\le [I(V;Y|US)-I(V;Z|US)]^+.\}.
\end{aligned}$$

Furthermore, set

$$\begin{aligned}
\mathcal{R}_{\rm s}^{(\rm in)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,V,X,S)\in\mathcal{Q}_1} \mathcal{R}(U,V,X,S|\Gamma),\\
\mathcal{R}_{\rm s}^{(\rm out)}(\Gamma) &\stackrel{\triangle}{=} \bigcup_{(U,V,X,S)\in\mathcal{Q}_2} \mathcal{R}(U,V,X,S|\Gamma).
\end{aligned}$$

Our capacity results in the case of stochastic encoding are as follows.

Theorem 4: For any relay channel Γ,

$$\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma)\subseteq\mathcal{R}_{\rm s}(\Gamma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma).$$

Theorem 5: For any relay channel Γ,

$$\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma)\subseteq\mathcal{R}_{\rm s}^{(\rm in)}(\Gamma)\subseteq\mathcal{R}_{\rm s}(\Gamma)\subseteq\mathcal{R}_{\rm s}^{(\rm out)}(\Gamma).$$

The above two theorems together with arguments similar to those in the case of deterministic coding yield the following three corollaries.

Corollary 4: If the the relay channel Γ is reversely degraded,

$$\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma)=\mathcal{R}_{\rm s}(\Gamma)=\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma).$$

Corollary 5: If the relay channel Γ is semi deterministic,

$$\mathcal{R}_{\rm s}^{(\rm in)}(\Gamma)=\mathcal{R}_{\rm s}(\Gamma)=\mathcal{R}_{\rm s}^{(\rm out)}(\Gamma).$$

Corollary 6: If the relay channel Γ is degraded, then no security on the private messages is guaranteed even if f_n is a stochastic encoder.

When $|\mathcal{S}|=1$, the reversely degraded relay channel becomes the degraded broadcast channel. Wyner [4] discussed the wire-tap channel in the case of degraded broadcast channels. Corollary 4 can be regarded as an extension of his result to the case where wire-tapper may assist the transmission of common messages. Corollary 6 meets our intuition in the sense that if the relay channel is degraded, the relay can do anything that the destination can.

C. Stochastic Relay Function

In this subsection we state our results in the case where the relay may use a stochastic encoder. Let $\mathcal{R}_{\rm d}^*(\Gamma)$ and $\mathcal{R}_{\rm s}^*(\Gamma)$ be denoted by the deterministic and stochastic rate equivocation regions, respectively, in the case where the stochastic relay encoder may be used. It is obvious that $\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma)$ and $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma)$ still serve as inner bounds of $\mathcal{R}_{\rm d}^*(\Gamma)$. Similarly, $\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma)$ and $\mathcal{R}_{\rm s}^{(\rm in)}(\Gamma)$ serve as inner bounds of $\mathcal{R}_{\rm s}^*(\Gamma)$. Our capacity results on outer bounds in the case of stochastic relay encoder are described in the following theorem.

Theorem 6: If Γ belongs to the class NL, $\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$, $\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$, and $\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$ still serve as outer bounds of $\mathcal{R}_{\rm d}^*(\Gamma)$. Similarly, if Γ belongs to the class NL, $\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma)$ and $\mathcal{R}_{\rm s}^{(\rm out)}(\Gamma)$ still serve as outer bounds of $\mathcal{R}_{\rm s}^*(\Gamma)$.

IV. Secrecy Capacities of the RCC

In this section we derive explicit inner and outer bounds of the secrecy capacity region by using the results in the previous section. We first consider the special case of no common message. Define

$$\begin{aligned}
\mathcal{R}_{\rm d1e}(\Gamma) &\stackrel{\triangle}{=} \{(R_1,R_{\rm e}): (0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(\Gamma)\},\\
\mathcal{R}_{\rm s1e}(\Gamma) &\stackrel{\triangle}{=} \{(R_1,R_{\rm e}): (0,R_1,R_{\rm e})\in\mathcal{R}_{\rm s}(\Gamma)\}.
\end{aligned}$$

To state a result on $\mathcal{R}_{\rm d1e}(\Gamma)$ and $\mathcal{R}_{\rm s1e}(\Gamma)$ set

$$\begin{aligned}
\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_1,R_{\rm e}) : R_1, R_{\rm e} \ge 0\,,\\
&R_1 \le I(X;Y|US)\,,\\
&R_{\rm e} \le [R_1 - I(X;Z|US)]^+ .\}\,,\\
\tilde{\mathcal{R}}^{(\rm out)}_{\rm d1e}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_1,R_{\rm e}) : R_1, R_{\rm e} \ge 0\,,\\
&R_1 \le I(X;YZ|US)\,,\\
&R_{\rm e} \le [R_1 - I(X;Z|US)]^+ .\}\,,\\
\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_1,R_{\rm e}) : R_1, R_{\rm e} \ge 0\,,\\
&R_{\rm e} \le R_1 \le I(X;Y|US)\,,\\
&R_{\rm e} \le [I(X;Y|US)\\
&\qquad -I(X;Z|US)]^+ .\}\,,\\
\tilde{\mathcal{R}}^{(\rm out)}_{\rm s1e}(U,X,S|\Gamma) \stackrel{\triangle}{=} \{&(R_1,R_{\rm e}) : R_1, R_{\rm e} \ge 0\,,\\
&R_{\rm e} \le R_1 \le I(X;YZ|US)\,,\\
&R_{\rm e} \le I(X;Y|ZUS)\,.\}\,,\\
\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(\Gamma) \stackrel{\triangle}{=} &\bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(U,X,S|\Gamma)\,,\\
\tilde{\mathcal{R}}^{(\rm out)}_{\rm d1e}(\Gamma) \stackrel{\triangle}{=} &\bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}^{(\rm out)}_{\rm d1e}(U,X,S|\Gamma)\,,\\
\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(\Gamma) \stackrel{\triangle}{=} &\bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(U,X,S|\Gamma)\,,\\
\tilde{\mathcal{R}}^{(\rm out)}_{\rm s1e}(\Gamma) \stackrel{\triangle}{=} &\bigcup_{(U,X,S)\in\mathcal{P}_1} \tilde{\mathcal{R}}^{(\rm out)}_{\rm s1e}(U,X,S|\Gamma)\,.
\end{aligned}$$

From Theorems 1 and 4, we have the following corollary.

Corollary 7: For any relay channel Γ,

$$\begin{aligned}
\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(\Gamma) \subseteq \mathcal{R}_{\rm d1e}(\Gamma) \subseteq \tilde{\mathcal{R}}^{(\rm out)}_{\rm d1e}(\Gamma)\,,\\
\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(\Gamma) \subseteq \mathcal{R}_{\rm s1e}(\Gamma) \subseteq \tilde{\mathcal{R}}^{(\rm out)}_{\rm s1e}(\Gamma)\,.
\end{aligned}$$

In particular, if Γ is reversely degraded,

$$\begin{aligned}
\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(\Gamma) = \mathcal{R}_{\rm d1e}(\Gamma) = \tilde{\mathcal{R}}^{(\rm out)}_{\rm d1e}(\Gamma),\\
\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(\Gamma) = \mathcal{R}_{\rm s1e}(\Gamma) = \tilde{\mathcal{R}}^{(\rm out)}_{\rm s1e}(\Gamma).
\end{aligned}$$

Now we consider the case where Γ is reversely degraded. In this case we compare $\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(\Gamma) = \mathcal{R}_{\rm d1e}(\Gamma)$ and $\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(\Gamma) = \mathcal{R}_{\rm s1e}(\Gamma)$. The regions $\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(U,X,S|\Gamma)$ and $\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(U,X,S|\Gamma)$ in this case are shown in Fig. 3. It can be seen from this figure that the region $\tilde{\mathcal{R}}^{(\rm in)}_{\rm d1e}(U,X,S|\Gamma)$ is strictly smaller than $\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(U,X,S|\Gamma)$. In $\tilde{\mathcal{R}}^{(\rm in)}_{\rm s1e}(U,X,S|\Gamma)$, the point $(R_1^*, R_{\rm e}^*)$ whose components are given by

$$R_1^* = R_{\rm e}^* = I(X;Y|US) - I(X;Z|US) \tag{7}$$

belongs to $\mathcal{R}_{\rm s1e}(\Gamma)$. This implies that the relay is kept completely ignorant of the private message. In this case we say that the perfect secrecy on the private message is established. The stochastic secrecy capacity region $\mathcal{C}_{\rm ss}(\Gamma)$ and the secrecy capacity $C_{\rm ss}(\Gamma)$ for the RCC are defined by

$$\begin{aligned}
\mathcal{C}_{\rm ss}(\Gamma) \stackrel{\triangle}{=} \{(R_0,R_1) : (R_0,R_1,R_1) \in \mathcal{R}_{\rm s}(\Gamma)\}\,,\\
C_{\rm ss}(\Gamma) \stackrel{\triangle}{=} \max_{(R_1,R_1)\in\mathcal{R}_{\rm s1e}(\Gamma)} R_1 = \max_{(0,R_1)\in\mathcal{C}_{\rm ss}(\Gamma)} R_1\,.
\end{aligned}$$

On the other hand, if we require the perfect secrecy in the case of deterministic encoding, we must have $R_1 = R_{\rm e}$ for $(R_1,R_{\rm e}) \in \mathcal{R}_{\rm d1e}(\Gamma)$. Then, it follows from Corollary 7 that if Γ is reversely degraded, we must have

$$I(X,Z|US) = 0 \text{ for } (U,X,Y) \in \mathcal{P}_1. \tag{8}$$

This condition is very hard to hold in general. Thus the prefect secrecy on private message can seldom be attained by the deterministic encoding. Another criterion of comparing $\mathcal{R}_{\rm d}(\Gamma)$ and $\mathcal{R}_{\rm s}(\Gamma)$ is the maximum equivocation rate in the rate-equivocation region. For $\mathcal{R}_{\rm d}(\Gamma)$ and $\mathcal{R}_{\rm s}(\Gamma)$, those are formally defined by

$$C_{\rm de}(\Gamma) \stackrel{\triangle}{=} \max_{\substack{(R_0,R_1,R_{\rm e})\\ \in\mathcal{R}_{\rm d}(\Gamma)}} R_{\rm e} \text{ and } C_{\rm se}(\Gamma) \stackrel{\triangle}{=} \max_{\substack{(R_0,R_1,R_{\rm e})\\ \in\mathcal{R}_{\rm s}(\Gamma)}} R_{\rm e},$$

respectively. We describe our results on $\mathcal{C}_{\rm ss}(\Gamma)$, $C_{\rm de}(\Gamma)$, $C_{\rm ss}(\Gamma)$, and $C_{\rm se}(\Gamma)$ which are obtained as corollaries of Theorems 1 and 4. Set

$$\begin{aligned}
\tilde{\mathcal{C}}^{(\rm in)}_{\rm ss}(\Gamma) \stackrel{\triangle}{=} \{&(R_0,R_1) : R_0, R_1 \ge 0\,,\\
&R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,,\\
&R_1 \le [I(X;Y|US) - I(X;Z|US)]^+\,,\\
&\text{for some } (U,X,S) \in \mathcal{P}_1 .\}\,,\\
\tilde{\mathcal{C}}^{(\rm out)}_{\rm ss}(\Gamma) \stackrel{\triangle}{=} \{&(R_0,R_1) : R_0, R_1 \ge 0\,,\\
&R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,,\\
&R_1 \le I(X;Y|ZUS)\,,\\
&\text{for some } (U,X,S) \in \mathcal{P}_1 .\}\,.
\end{aligned}$$

Then we have the following.

Corollary 8: For any relay channel Γ,

$$\tilde{\mathcal{C}}^{(\rm in)}_{\rm ss}(\Gamma) \subseteq \mathcal{C}_{\rm ss}(\Gamma) \subseteq \tilde{\mathcal{C}}^{(\rm out)}_{\rm ss}(\Gamma)\,.$$

Furthermore, we have

$$\begin{aligned}
&\max_{(X,S)} [I(X;Y|S) - I(X;Z|S)]^+\\
&\le \max_{(U,X,S)\in\mathcal{P}_1} [I(X;Y|US) - I(X;Z|US)]^+\\
&\le C_{\rm de}(\Gamma) \le C_{\rm ss}(\Gamma) \le C_{\rm se}(\Gamma)\\
&\le \max_{(U,X,S)\in\mathcal{P}_1} I(X;Y|ZUS) = \max_{(X,S)} I(X;Y|ZS)\,.
\end{aligned}$$

In particular, if Γ is reversely degraded, we have

$$\tilde{\mathcal{C}}^{(\rm in)}_{\rm ss}(\Gamma) = \mathcal{C}_{\rm ss}(\Gamma) = \tilde{\mathcal{C}}^{(\rm out)}_{\rm ss}(\Gamma)$$

and

$$\begin{aligned}
C_{\rm de}(\Gamma) = C_{\rm ss}(\Gamma) = C_{\rm se}(\Gamma)\\
= \max_{(X,S)} [I(X;Y|S) - I(X;Z|S)]\,.
\end{aligned}$$

Typical shapes of the regions $\mathcal{R}_{\rm d1e}(\Gamma)$ and $\mathcal{R}_{\rm s1e}(\Gamma)$ in the case of reversely degraded relay channels are shown in Fig. 4. The secrecy capacity $C_{\rm ss}(\Gamma)$ is also shown in this figure. Next, we state a result which is obtained as a corollary of Theorems

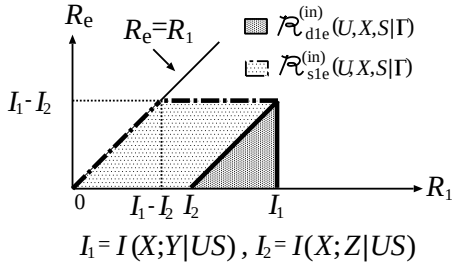

Fig. 3. The regions $\tilde{\mathcal{R}}^{(\mathrm{in})}_{\mathrm{d1e}}(U,X,S|\Gamma)$ and $\tilde{\mathcal{R}}^{(\mathrm{in})}_{\mathrm{s1e}}(U,X,S|\Gamma)$.

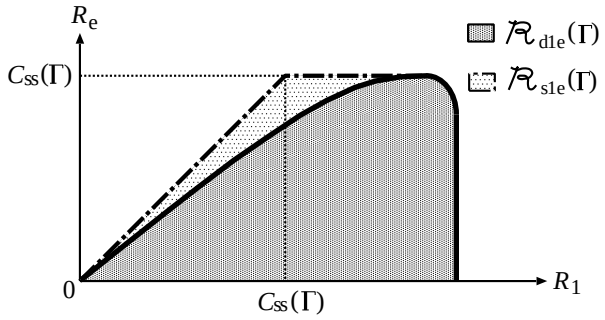

Fig. 4. The regions $\mathcal{R}_{\mathrm{d1e}}(\Gamma)=\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(\Gamma)$ and $\mathcal{R}_{\mathrm{s1e}}(\Gamma)=\mathcal{R}^{(\mathrm{in})}_{\mathrm{s1e}}(\Gamma)$ and $C_{\mathrm{ss}}(\Gamma)=C_{\mathrm{de}}(\Gamma)=C_{\mathrm{se}}(\Gamma)$ for the reversely degraded relay channels.

2 and 5. To state this result, set

$$
\begin{aligned}
&\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(U,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \mathcal{R}^{(\mathrm{in})}_{\mathrm{d}}(U,X,S|\Gamma)\cap\{(R_0,R_1,R_{\mathrm{e}}):R_0=0\}\\
&= \{(R_1,R_{\mathrm{e}}):R_1,R_{\mathrm{e}}\ge 0\,,\\
&\quad R_1\le I(X;Y|US)+\min\{I(US;Y),I(U;Z|S)\}\,,\\
&\quad R_{\mathrm{e}}\le [R_1-I(X;Z|US)]^+\,,\\
&\quad R_{\mathrm{e}}\le [I(X;Y|US)-I(X;Z|US)]^+\,.\},\\
&\quad \mathcal{R}^{(\mathrm{out})}_{\mathrm{d1e}}(U,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \mathcal{R}^{(\mathrm{out})}_{\mathrm{d}}(U,X,S|\Gamma)\cap\{(R_0,R_1,R_{\mathrm{e}}):R_0=0\}\\
&= \{(R_1,R_{\mathrm{e}}):R_1,R_{\mathrm{e}}\ge 0\,,\\
&\quad R_1\le I(X;Y|US)+\min\{I(U;Z|S),I(US;Y)\}\,,\\
&\quad R_{\mathrm{e}}\le [R_1-I(X;Z|US)+I(U;Z|XS)]^+\,,\\
&\quad R_{\mathrm{e}}\le [I(X;Y|US)-I(X;Z|US)]^+\,.\},\\
&\quad \mathcal{R}_{1\mathrm{e}}(U,V,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \mathcal{R}(U,V,X,S|\Gamma)\cap\{(R_0,R_1,R_{\mathrm{e}}):R_0=0\}\\
&= \{(R_1,R_{\mathrm{e}}):0\le R_{\mathrm{e}}\le R_1\,,\\
&\quad R_1\le I(V;Y|US)+\min\{I(US;Y),I(U;Z|S)\}\,,\\
&\quad R_{\mathrm{e}}\le [I(V;Y|US)-I(V;Z|US)]^+\,.\},\\
&\quad \mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,X,S)\in\mathcal{Q}_1}\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(U,X,S|\Gamma)\,,\\
&\quad \mathcal{R}^{(\mathrm{out})}_{\mathrm{d1e}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,X,S)\in\mathcal{Q}_2}\mathcal{R}^{(\mathrm{out})}_{\mathrm{d1e}}(U,X,S|\Gamma)\,,\\
&\quad \mathcal{R}^{(\mathrm{in})}_{\mathrm{s1e}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,V,X,S)\in\mathcal{Q}_1}\mathcal{R}_{1\mathrm{e}}(U,V,X,S|\Gamma)\,,\\
&\quad \mathcal{R}^{(\mathrm{out})}_{\mathrm{s1e}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,V,X,S)\in\mathcal{Q}_2}\mathcal{R}_{1\mathrm{e}}(U,V,X,S|\Gamma)\,.
\end{aligned}
$$

Furthermore, set

$$
\begin{aligned}
&\mathcal{C}_{\mathrm{s}}(U,V,X,S|\Gamma)\\
&\stackrel{\triangle}{=} \mathcal{R}(U,V,X,S|\Gamma)\cap\{(R_0,R_1,R_{\mathrm{e}}):R_1=R_{\mathrm{e}}\}\\
&= \{(R_0,R_1):R_0,R_1\ge 0\,,\\
&\quad R_0\le\min\{I(US;Y),I(U;Z|S)\}\,,\\
&\quad R_1\le [I(V;Y|US)-I(V;Z|US)]^+\,\},\\
&\quad \mathcal{C}^{(\mathrm{in})}_{\mathrm{ss}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,V,X,S)\in\mathcal{Q}_1}\mathcal{C}_{\mathrm{s}}(U,V,X,S|\Gamma)\,,\\
&\quad \mathcal{C}^{(\mathrm{out})}_{\mathrm{ss}}(\Gamma)\stackrel{\triangle}{=}\bigcup_{(U,V,X,S)\in\mathcal{Q}_2}\mathcal{C}_{\mathrm{s}}(U,V,X,S|\Gamma)\,.
\end{aligned}
$$

From Theorems 2 and 5, we have the following corollary.

Corollary 9: For any relay channel Γ,

$$
\begin{aligned}
&\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(\Gamma)\subseteq\mathcal{R}_{\mathrm{d1e}}(\Gamma)\subseteq\mathcal{R}^{(\mathrm{out})}_{\mathrm{d1e}}(\Gamma)\subseteq\mathcal{R}^{(\mathrm{out})}_{\mathrm{s1e}}(\Gamma)\,,\\
&\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(\Gamma)\subseteq\mathcal{R}^{(\mathrm{in})}_{\mathrm{s1e}}(\Gamma)\subseteq\mathcal{R}_{\mathrm{s1e}}(\Gamma)\subseteq\mathcal{R}^{(\mathrm{out})}_{\mathrm{s1e}}(\Gamma)\,,\\
&\mathcal{C}^{(\mathrm{in})}_{\mathrm{ss}}(\Gamma)\subseteq\mathcal{C}_{\mathrm{ss}}(\Gamma)\subseteq\mathcal{C}^{(\mathrm{out})}_{\mathrm{ss}}(\Gamma)\,.
\end{aligned}
$$

Furthermore,

$$
\begin{aligned}
&\max_{(U,X,S)\in\mathcal{P}_1}[I(X;Y|US)-I(X;Z|US)]^+\\
&\le C_{\mathrm{de}}(\Gamma)\\
&\le \max_{(U,X,S)\in\mathcal{P}_2}[I(V;Y|US)-I(V;Z|US)]^+\,,\\
&\quad \max_{(U,V,X,S)\in\mathcal{Q}_1}[I(V;Y|US)-I(V;Z|US)]^+\\
&\le C_{\mathrm{ss}}(\Gamma)\le C_{\mathrm{se}}(\Gamma)\\
&\le \max_{(U,V,X,S)\in\mathcal{Q}_2}[I(V;Y|US)-I(V;Z|US)]^+\,.
\end{aligned}
$$

If Γ is semi deterministic, then

$$
\begin{aligned}
\mathcal{R}^{(\mathrm{in})}_{\mathrm{d1e}}(\Gamma)=\mathcal{R}_{\mathrm{d1e}}(\Gamma)=\mathcal{R}^{(\mathrm{out})}_{\mathrm{d1e}}(\Gamma)\,,\\
\mathcal{R}^{(\mathrm{in})}_{\mathrm{s1e}}(\Gamma)=\mathcal{R}_{\mathrm{s1e}}(\Gamma)=\mathcal{R}^{(\mathrm{out})}_{\mathrm{s1e}}(\Gamma)\,,\\
\mathcal{C}^{(\mathrm{in})}_{\mathrm{ss}}(\Gamma)=\mathcal{C}_{\mathrm{ss}}(\Gamma)=\mathcal{C}^{(\mathrm{out})}_{\mathrm{ss}}(\Gamma)\,.
\end{aligned}
$$

Furthermore,

$$
\begin{aligned}
C_{\mathrm{de}}(\Gamma)&=\max_{(U,X,S)\in\mathcal{P}_1}[I(X;Y|US)-I(X;Z|US)]^+\,,\\
C_{\mathrm{ss}}(\Gamma)&=C_{\mathrm{se}}(\Gamma)\\
&=\max_{(U,V,X,S)\in\mathcal{Q}_1}[I(V;Y|US)-I(V;Z|US)]^+\,.
\end{aligned}
$$

It can be seen from the above corollary that $C_{\mathrm{se}}(\Gamma)$ may strictly be larger than $C_{\mathrm{de}}(\Gamma)$ unless Γ is reversely degraded. By a simple analytical argument we can show that $C^{(\mathrm{in})}_{\mathrm{ss}}(\Gamma)$ can be attained by $S=s^*$, where $s^*\in\mathcal{S}$ is the best input alphabet which maximizes the secrecy rate

$$\max_{(V,U,X,S=s^*)\in\mathcal{Q}_1}\{I(V;Y|US=s^*)-I(V;Z|US=s^*)\}\,.$$

This implies that the coding strategy achieving $C^{(\mathrm{in})}_{\mathrm{ss}}(\Gamma)$ does not help improving the secrecy rate compared with the case where the relay is simply a wire-tapper, except that the relay may choose the best $S=s^*$ to benefit the receiver. Cover and El Gamal [24] introduced a transmission scheme of the relay called the compress-and-forward scheme, where the relay transmits a quantized version of its received signal. This

scheme is also applicable to the RCC. He and Yener [18], [19] derived an inner bound of $\mathcal{R}_{\rm s1e}(\Gamma)$ in the case where the relay employs the compress-and-forward scheme to show that the relay may improve the secrecy capacity.

V. Gaussian Relay Channels with Confidential Messages

In this section we study Gaussian relay channels with confidential messages, where two channel outputs are corrupted by additive white Gaussian noises. Let (ξ_1, ξ_2) be correlated zero mean Gaussian random vector with covariance matrix

$$\Sigma = \begin{pmatrix} N_1 & \rho\sqrt{N_1 N_2} \\ \rho\sqrt{N_1 N_2} & N_2 \end{pmatrix}, |\rho| < 1 .$$

Let $\{(\xi_{1,i}, \xi_{2,i})\}_{i=1}^{\infty}$ be a sequence of independent identically distributed (i.i.d.) zero mean Gaussian random vectors. Each $(\xi_{1,i}, \xi_{2,i})$ has the covariance matrix Σ. The Gaussian relay channel is specified by the above covariance matrix Σ. Two channel outputs Y_i and Z_i of the relay channel at the ith transmission are given by

$$Y_i = X_i + S_i + \xi_{1,i}\,, Z_i = X_i + \xi_{2,i}\,.$$

It is obvious that Σ belongs to the class NL. In this class of Gaussian relay channels we assume that the relay encoder $\{g_i\}_{i=1}$ is allowed to be stochastic. Since $(\xi_{1,i}, \xi_{2,i}), i = 1, 2, \cdots, n$ have the covariance matrix Σ, we have

$$\xi_{2,i} = \rho\sqrt{\frac{N_2}{N_1}}\xi_{1,i} + \xi_{2|1,i}\,,$$

where $\xi_{2|1,i}, i = 1, 2, \cdots, n$ are zero mean Gaussian random variable with variance $(1-\rho^2)N_2$ and independent of $\xi_{1,i}$. In particular if Σ satisfies $N_1 \le N_2$ and $\rho = \sqrt{\frac{N_1}{N_2}}$, we have for $i = 1, 2, \cdots, n$,

$$Y_i = X_i + S_i + \xi_{1,i}, Z_i = X_i + \xi_{1,i} + \xi_{2|1,i}$$

which implies that for $i = 1, 2, \cdots, n$, $Z_i \to (Y_i, S_i) \to X_i$. Hence, the Gaussian relay channel becomes reversely degraded relay channel. Two channel input sequences $\{X_i\}_{i=1}^n$ and $\{S_i\}_{i=1}^n$ are subject to the following average power constraints:

$$\frac{1}{n}\sum_{i=1}^{n}\mathbf{E}\left[X_i^2\right] \le P_1\,, \frac{1}{n}\sum_{i=1}^{n}\mathbf{E}\left[S_i^2\right] \le P_2\,.$$

Let $\mathcal{R}_{\rm d}(P_1, P_2|\Sigma)$ and $\mathcal{R}_{\rm s}(P_1, P_2|\Sigma)$ be rate-equivocation regions for the above Gaussian relay channel when we use deterministic and stochastic encoders, respectively. To state our results on $\mathcal{R}_{\rm d}(P_1, P_2|\Sigma)$ and $\mathcal{R}_{\rm s}(P_1, P_2|\Sigma)$, set

$$\begin{aligned}
&\mathcal{R}_{\rm d}^{(\rm in)}(P_1, P_2|\Sigma) \\
&\stackrel{\triangle}{=} \{(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \max_{0\le\eta\le 1}\min\left\{C\left(\frac{\bar\theta P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{\theta P_1 + N_1}\right)\right. , \\
&\qquad\qquad \left. C\left(\frac{\bar\theta\eta P_1}{\theta P_1 + N_2}\right)\right\}\,, \\
&\quad R_1 \le C\left(\frac{\theta P_1}{N_1}\right)\,, \\
&\quad R_{\rm e} \le \left[R_1 - C\left(\frac{\theta P_1}{N_2}\right)\right]^+\,, \\
&\qquad \text{for some } 0 \le \theta \le 1\,.\}\,, \\
&\mathcal{R}_{\rm d}^{(\rm out)}(P_1, P_2|\Sigma) \\
&\stackrel{\triangle}{=} \{(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \min\left\{C\left(\frac{\bar\theta P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{\theta P_1 + N_1}\right)\right. , \\
&\qquad\qquad \left. C\left(\frac{\bar\theta\eta P_1}{\theta P_1 + N_2}\right)\right\}\,, \\
&\quad R_1 \le C\left(\frac{\theta P_1}{\frac{(1-\rho^2)N_1 N_2}{N_1 + N_2 - 2\rho\sqrt{N_1 N_2}}}\right)\,, \\
&\quad R_0 + R_1 \le C\left(\frac{P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{N_1}\right)\,, \\
&\quad R_{\rm e} \le \left[R_1 - C\left(\frac{\theta P_1}{N_2}\right)\right]^+\,, \\
&\qquad \text{for some } 0 \le \theta \le 1, 0 \le \eta \le 1\,.\}\,,
\end{aligned}$$

where $C(x) \stackrel{\triangle}{=} \frac{1}{2}\log(1+x)$. Furthermore, set

$$\begin{aligned}
&\mathcal{R}_{\rm s}^{(\rm in)}(P_1, P_2|\Sigma) \\
&\stackrel{\triangle}{=} \{(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \max_{0\le\eta\le 1}\min\left\{C\left(\frac{\bar\theta P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{\theta P_1 + N_1}\right)\right. , \\
&\qquad\qquad \left. C\left(\frac{\bar\theta\eta P_1}{\theta P_1 + N_2}\right)\right\}\,, \\
&\quad R_{\rm e} \le R_1 \le C\left(\frac{\theta P_1}{N_1}\right)\,, \\
&\quad R_{\rm e} \le \left[C\left(\frac{\theta P_1}{N_1}\right) - C\left(\frac{\theta P_1}{N_2}\right)\right]^+\,, \\
&\qquad \text{for some } 0 \le \theta \le 1\,.\}\,, \\
&\mathcal{R}_{\rm s}^{(\rm out)}(P_1, P_2|\Sigma) \\
&\stackrel{\triangle}{=} \{(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\
&\quad R_0 \le \min\left\{C\left(\frac{\bar\theta P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{\theta P_1 + N_1}\right)\right. , \\
&\qquad\qquad \left. C\left(\frac{\bar\theta\eta P_1}{\theta P_1 + N_2}\right)\right\}\,, \\
&\quad R_0 + R_1 \le C\left(\frac{P_1 + P_2 + 2\sqrt{\bar\theta\bar\eta P_1 P_2}}{N_1}\right)\,, \\
&\quad R_{\rm e} \le R_1 \le C\left(\frac{\theta P_1}{\frac{(1-\rho^2)N_1 N_2}{N_1 + N_2 - 2\rho\sqrt{N_1 N_2}}}\right)\,, \\
&\quad R_{\rm e} \le \left[C\left(\frac{\theta P_1}{\frac{(1-\rho^2)N_1 N_2}{N_1 + N_2 - 2\rho\sqrt{N_1 N_2}}}\right) - C\left(\frac{\theta P_1}{N_2}\right)\right]^+\,, \\
&\qquad \text{for some } 0 \le \theta \le 1, 0 \le \eta \le 1\,.\}\,.
\end{aligned}$$

Our results are the followings.

Theorem 7: For any Gaussian relay channel Σ,

$$\mathcal{R}_{\rm d}^{\rm (in)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm d}^{\rm (out)}(P_1,P_2|\Sigma), \quad (9)$$
$$\mathcal{R}_{\rm s}^{\rm (in)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm s}^{\rm (out)}(P_1,P_2|\Sigma). \quad (10)$$

In particular, if the relay channel is reversely degraded, i.e., $N_1\le N_2$ and $\rho=\sqrt{\frac{N_1}{N_2}}$, then

$$\mathcal{R}_{\rm d}^{\rm (in)}(P_1,P_2|\Sigma)=\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)=\mathcal{R}_{\rm d}^{\rm (out)}(P_1,P_2|\Sigma)\,,$$
$$\mathcal{R}_{\rm s}^{\rm (in)}(P_1,P_2|\Sigma)=\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)=\mathcal{R}_{\rm s}^{\rm (out)}(P_1,P_2|\Sigma)\,.$$

Proof of the first inclusions in (9) and (10) in the above theorem is standard. The second inclusions in (9) and (10) can be proved by a converse coding argument similar to the one developed by Liang and Veeravalli [27]. Proof of Theorem 7 will be stated in Section VIII.

Next we study the secrecy capacity of the Gaussian RCCs. Define two regions by

$$\begin{aligned}&\mathcal{R}_{\rm d1e}(P_1,P_2|\Sigma)\\ \triangleq\ &\{(R_1,R_{\rm e}):(0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)\}\,,\\ &\mathcal{R}_{\rm s1e}(P_1,P_2|\Sigma)\\ \triangleq\ &\{(R_1,R_{\rm e}):(0,R_1,R_{\rm e})\in\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)\}\,.\end{aligned}$$

Furthermore, define the secrecy capacity region $\mathcal{C}_{\rm ss}(P_1,P_2|\Sigma)$ and the secrecy capacity $C_{\rm ss}(P_1,P_2|\Sigma)$ by

$$\begin{aligned}&\mathcal{C}_{\rm ss}(P_1,P_2|\Sigma)\\ \triangleq\ &\{(R_0,R_1):(R_0,R_1,R_1)\in\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)\}\,.\\ &C_{\rm ss}(P_1,P_2|\Sigma)\\ \triangleq\ &\max_{(R_1,R_1)\in\mathcal{R}_{\rm s1e}(P_1,P_2|\Sigma)}R_1=\max_{(0,R_1)\in\mathcal{C}_{\rm ss}(P_1,P_2|\Sigma)}R_1\,.\end{aligned}$$

Maximum equivocation rates for $\mathcal{R}_{\rm d}(P_1,\ P_2|\Sigma)$ and $\mathcal{R}_{\rm s}(P_1,\ P_2|\Sigma)$ are defined by

$$\begin{aligned}C_{\rm de}(P_1,P_2|\Sigma)&\triangleq\max_{(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)}R_{\rm e}\,,\\ C_{\rm se}(P_1,P_2|\Sigma)&\triangleq\max_{(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)}R_{\rm e}\,.\end{aligned}$$

Set

$$\begin{aligned}\mathcal{R}_{\rm d1e}^{\rm (in)}(P_1|\Sigma)\triangleq\ &\{(R_1,R_{\rm e}):R_1,R_{\rm e}\ge0\,,\\ &R_1\le C\left(\tfrac{\theta P_1}{N_1}\right),\\ &R_{\rm e}\le\left[R_1-C\left(\tfrac{\theta P_1}{N_2}\right)\right]^+,\\ &\quad\text{for some }0\le\theta\le1\,.\}\,,\\ \mathcal{R}_{\rm d1e}^{\rm (out)}(P_1|\Sigma)\triangleq\ &\{(R_1,R_{\rm e}):R_1,R_{\rm e}\ge0\,,\\ &R_1\le C\left(\frac{\theta P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right),\\ &R_{\rm e}\le\left[R_1-C\left(\tfrac{\theta P_1}{N_2}\right)\right]^+,\\ &\quad\text{for some }0\le\theta\le1\,.\}\,,\end{aligned}$$

$$\begin{aligned}\mathcal{R}_{\rm s1e}^{\rm (in)}(P_1|\Sigma)\triangleq\ &\{(R_1,R_{\rm e}):R_1,R_{\rm e}\ge0\,,\\ &R_{\rm e}\le R_1\le C\left(\tfrac{P_1}{N_1}\right),\\ &R_{\rm e}\le\left[C\left(\tfrac{P_1}{N_1}\right)-C\left(\tfrac{P_1}{N_2}\right)\right]^+.\}\,,\end{aligned}$$

$$\begin{aligned}&\mathcal{R}_{\rm s1e}^{\rm (out)}(P_1|\Sigma)\\ \triangleq\ &\{(R_1,R_{\rm e}):R_1,R_{\rm e}\ge0\,,\\ &R_{\rm e}\le R_1\le C\left(\frac{P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right),\\ &R_{\rm e}\le\left[C\left(\frac{P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right)-C\left(\tfrac{P_1}{N_2}\right)\right]^+.\}\,.\end{aligned}$$

Furthermore, set

$$\begin{aligned}&\mathcal{C}_{\rm ss}^{\rm (in)}(P_1,P_2|\Sigma)\\ \triangleq\ &\{(R_0,R_1):R_0,R_1\ge0\,,\\ &R_0\le\max_{0\le\eta\le1}\min\left\{C\left(\tfrac{\bar\theta P_1+P_2+2\sqrt{\bar\theta\bar\eta P_1P_2}}{\theta P_1+N_1}\right),\right.\\ &\qquad\left.C\left(\tfrac{\bar\theta\eta P_1}{\theta P_1+N_2}\right)\right\},\\ &R_1\le\left[C\left(\tfrac{\theta P_1}{N_1}\right)-C\left(\tfrac{\theta P_1}{N_2}\right)\right]^+,\\ &\quad\text{for some }0\le\theta\le1\,.\}\,,\end{aligned}$$

$$\begin{aligned}&\mathcal{C}_{\rm ss}^{\rm (out)}(P_1,P_2|\Sigma)\\ \triangleq\ &\{(R_0,R_1):R_0,R_1\ge0\,,\\ &R_0\le\max_{0\le\eta\le1}\min\left\{C\left(\tfrac{\bar\theta P_1+P_2+2\sqrt{\bar\theta\bar\eta P_1P_2}}{\theta P_1+N_1}\right),\right.\\ &\qquad\left.C\left(\tfrac{\bar\theta\eta P_1}{\theta P_1+N_2}\right)\right\},\\ &R_1\le\left[C\left(\frac{\theta P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right)-C\left(\tfrac{\theta P_1}{N_2}\right)\right]^+,\\ &\quad\text{for some }0\le\theta\le1\,.\}\,.\end{aligned}$$

We obtain the following two results as a corollary of Theorem 7.

Corollary 10: For any Gaussian relay channel Σ,

$$\mathcal{R}_{\rm d1e}^{\rm (in)}(P_1|\Sigma)\subseteq\mathcal{R}_{\rm d1e}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm d1e}^{\rm (out)}(P_1|\Sigma)\,,$$
$$\mathcal{R}_{\rm s1e}^{\rm (in)}(P_1|\Sigma)\subseteq\mathcal{R}_{\rm s1e}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm s1e}^{\rm (out)}(P_1|\Sigma)\,.$$

In particular, if $N_1\le N_2$ and $\rho=\sqrt{\frac{N_1}{N_2}}$, the regions $\mathcal{R}_{\rm d1e}(P_1,\ P_2|\Sigma)$ and $\mathcal{R}_{\rm s1e}(P_1,\ P_2|\Sigma)$ do not depend on P_2 and

$$\mathcal{R}_{\rm d1e}^{\rm (in)}(P_1|\Sigma)=\mathcal{R}_{\rm d1e}(P_1|\Sigma)=\mathcal{R}_{\rm d1e}^{\rm (out)}(P_1|\Sigma)\,,$$
$$\mathcal{R}_{\rm s1e}^{\rm (in)}(P_1|\Sigma)=\mathcal{R}_{\rm s1e}(P_1|\Sigma)=\mathcal{R}_{\rm s1e}^{\rm (out)}(P_1|\Sigma)\,.$$

Corollary 11: For any Gaussian relay channel Σ,

$$\mathcal{C}_{\rm ss}^{\rm (in)}(P_1,P_2|\Sigma)\subseteq\mathcal{C}_{\rm ss}(P_1,P_2|\Sigma)\subseteq\mathcal{C}_{\rm ss}^{\rm (out)}(P_1,P_2|\Sigma)\,.$$

Furthermore,

$$\begin{aligned}&\left[C\left(\tfrac{P_1}{N_1}\right)-C\left(\tfrac{P_1}{N_2}\right)\right]^+\\ \le\ &C_{\rm de}(P_1,P_2|\Sigma)\le C_{\rm ss}(P_1,P_2|\Sigma)\le C_{\rm se}(P_1,P_2|\Sigma)\\ \le\ &\left[C\left(\frac{P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right)-C\left(\tfrac{P_1}{N_2}\right)\right]^+.\end{aligned}$$

In particular, if $N_1\le N_2$ and $\rho=\sqrt{\frac{N_1}{N_2}}$,

$$\mathcal{C}_{\rm ss}^{\rm (in)}(P_1,P_2|\Sigma)=\mathcal{C}_{\rm ss}(P_1,P_2|\Sigma)=\mathcal{C}_{\rm ss}^{\rm (out)}(P_1,P_2|\Sigma)$$

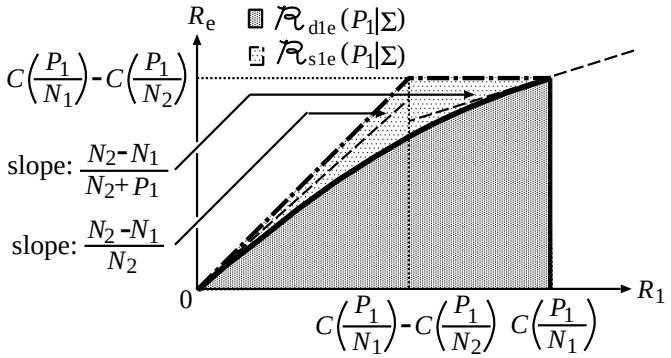

Fig. 5. Shapes of $\mathcal{R}_{\rm d1e}(P_1|\Sigma)$ and $\mathcal{R}_{\rm s1e}(P_1|\Sigma)$ for the reversely degraded relay channel Σ.

and

$$C_{\rm de}(P_1,P_2|\Sigma)=C_{\rm ss}(P_1,P_2|\Sigma)=C_{\rm se}(P_1,P_2|\Sigma)$$
$$=C\left(\tfrac{P_1}{N_1}\right)-C\left(\tfrac{P_1}{N_2}\right).$$

Typical shapes of $\mathcal{R}_{\rm d1e}(P_1|\Sigma)$ and $\mathcal{R}_{\rm s1e}(P_1|\Sigma)$ for the reversely degraded relay channel Σ are shown in Fig. 5. Note that the secrecy capacity $C_{\rm ss}(P_1,P_2|\Sigma)$ for the reversely degraded relay channel does not depend on the power constraint P_2 at the relay. This implies that the security of private messages is not affected by the relay. Leung-Yan-Cheong and Hellman [29] determined the secrecy capacity for the Gaussian wire-tap channel. The above secrecy capacity is equal to the secrecy capacity of the Gaussian wire-tap channel derived by them.

VI. Derivations of the Inner Bounds

In this section we prove Theorem 1, and the inclusion $\mathcal{R}_{\rm s}^{\rm (in)}(\Gamma)\subseteq\mathcal{R}_{\rm s}(\Gamma)$ in Theorem 5.

A. Encoding and Decoding Scheme

We first state an important lemma to derive inner bounds. To describe this lemma, we need some preparations. Let $\mathcal{T}_n$, $\mathcal{J}_n$, and $\mathcal{L}_n$ be three message sets to be transmitted by the sender. Let T_n,J_n, and L_n be uniformly distributed random variable on $\mathcal{T}_n$, $\mathcal{J}_n$, and $\mathcal{L}_n$, respectively. Elements of $\mathcal{T}_n$ are directed to the receiver and relay. Encoder function f_n is a one to one mapping from $\mathcal{T}_n\times\mathcal{J}_n\times\mathcal{L}_n$ to $\mathcal{X}^n$. Using the decoder function ψ_n, the receiver outputs an element of $\mathcal{T}_n\times\mathcal{J}_n\times\mathcal{L}_n$ from a received message of $\mathcal{Y}^n$. Using the decoder function φ_n, the relay outputs an element of $\mathcal{T}_n$ from a received message of $\mathcal{Z}^n$. Formal definitions of ψ_n and φ_n are $\psi_n:\mathcal{Y}^n\to\mathcal{T}_n\times\mathcal{J}_n\times\mathcal{L}_n$, $\varphi_n:\mathcal{Z}^n\to\mathcal{T}_n$. Error probabilities of decoding at the receiver and the relay are defined by

$$\mu_1^{(n)}\triangleq\Pr\{\psi_n(Y^n)\neq(T_n,J_n,L_n)\}\text{ and}$$
$$\mu_2^{(n)}\triangleq\Pr\{\varphi_n(Z^n)\neq T_n\},$$

respectively. The following is a key result to derive inner bounds of $\mathcal{R}_{\rm d}(\Gamma)$ and $\mathcal{R}_{\rm s}(\Gamma)$.

Lemma 1: Choose $(U,X,S)\in\mathcal{P}_1$ such that $I(X;Y\,|US)\geq I(X;Z|US)$. Then, there exists a sequence of quadruples $\{(f_n,\{g_i\}_{i=1}^n,\psi_n,\varphi_n)\}_{n=1}^\infty$ such that

$$\lim_{n\to\infty}\mu_1^{(n)}=\lim_{n\to\infty}\mu_2^{(n)}=0\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{T}_n|=\min\{I(US;Y),I(U;Z|S)\}\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{J}_n|=I(X;Y|US)\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{L}_n|=I(X;Y|US)-I(X;Z|US)\,,$$
$$\lim_{n\to\infty}\frac{1}{n}H(L_n|Z^n)\geq I(X;Y|US)-I(X;Z|US)\,.$$

In this subsection we give an encoding and decoding scheme which attains the transmission and equivocation rates described in Lemma 1. Let

$$\mathcal{T}_n=\{1,2,\cdots,2^{\lfloor nR_0\rfloor}\},\quad \mathcal{L}_n=\{1,2,\cdots,2^{\lfloor nr_1\rfloor}\},$$
$$\mathcal{J}_n=\{1,2,\cdots,2^{\lfloor nr_2\rfloor}\},$$

where $\lfloor x\rfloor$ stands for the integer part of x for $x>0$. We consider a transmission over B blocks, each with length n. For each $i=1,2,\cdots,B$, let $(t_i,j_i,l_i)\in\mathcal{T}_n\times\mathcal{J}_n\times\mathcal{L}_n$ be a triple of messages to be transmitted at the ith block. A sequence of $B-1$ message triples (t_i,j_i,l_i), $i=1,2,\cdots,B-1$ are sent over the channel in nB transmission. For $i=0$, the constant message pair $(t_0,j_0,l_0)=(1,1,1)$ is transmitted. For fixed n, the rate triple $(R_0\frac{B-1}{B},r_1\frac{B-1}{B},r_2\frac{B-1}{B})$ approaches (R_0,r_1,r_2) as $B\to\infty$.

We use random codes for the proof. Fix a joint probability distribution of (U,S,X,Y,Z):

$$p_{USXYZ}(u,s,x,y,z)$$
$$=p_S(s)p_{U|S}(u|s)p_{X|US}(x|u,s)\Gamma(y,z|x,s)\,,$$

where U is an auxiliary random variable that stands for the information being carried by the message to be sent to the receiver and the relay.

Random Codebook Generation: We generate a random code book by the following steps.

1. Set $\mathcal{W}_n\triangleq\{1,2,\cdots,2^{\lfloor nr\rfloor}\}$. Generate $2^{\lfloor nr\rfloor}$ i.i.d. $\boldsymbol{s}\in\mathcal{S}^n$ each with distribution $\prod_{i=1}^n p_S(s_i)$. Index $\boldsymbol{s}(w),w\in\mathcal{W}_n$.
2. For each $\boldsymbol{s}(w)$, generate $2^{\lfloor nR_0\rfloor}$ i.i.d. $\boldsymbol{u}\in\mathcal{U}^n$ each with distribution $\prod_{i=1}^n p_U(u_i|s_i)$. Index $\boldsymbol{u}(w,t)$, $t\in\mathcal{T}_n$.
3. For each $\boldsymbol{s}(w)$ and $\boldsymbol{u}(w,t)$, generate $2^{\lfloor nr_1\rfloor}\cdot2^{\lfloor nr_2\rfloor}$ i.i.d. $\boldsymbol{x}\in\mathcal{X}^n$ each with distribution $\prod_{i=1}^n p_{X|US}(x_i\,|u_i,s_i)$. Index $\boldsymbol{x}(w,t,j,l)$, $(w,t,j,l)\in\mathcal{W}_n\times\mathcal{T}_n\times\mathcal{J}_n\times\mathcal{L}_n$.

Random Partition of $\mathcal{T}_n$: We define the mapping $\phi_n:\mathcal{T}_n\to\mathcal{W}_n$ in the following manner. For each $t\in\mathcal{T}_n$, choose $w\in\mathcal{W}_n$ at random according to the uniform distribution on $\mathcal{W}_n$ and map t to w. The random choice is independent for each $t\in\mathcal{T}_n$. For each $w\in\mathcal{W}_n$, define $\mathcal{T}_n(w)\triangleq\{t\in\mathcal{T}_n:\phi_n(t)=w\}$. The family of sets $\{\mathcal{T}_n(w)\}_{w\in\mathcal{W}_n}$ is a partition of $\mathcal{T}_n$.

Encoding: Let (t_i,j_i,l_i) be the new message triple to be sent from the sender in block i and $(t_{i-1},j_{i-1},l_{i-1})$ be the message triple to be sent from the sender in previous block $i-1$. At the beginning of block i, the sender computes $w_i=\phi_n(t_{i-1})$ and sends the codeword $\boldsymbol{x}(w_i,t_i,j_i,l_i)\in\mathcal{X}^n$.

At the beginning of block i, the relay has decoded the message t_{i-1}. It then computes $w_i = \phi_n(t_{i-1})$ and sends the codeword $\boldsymbol{s}(w_i) \in \mathcal{S}^n$.

Decoding: Let $\boldsymbol{y}_i \in \mathcal{Y}^n$ and $\boldsymbol{z}_i \in \mathcal{Z}^n$ be the sequences that the reviver and the relay obtain at the end of block i, respectively. The decoding procedures at the end of block i are as follows.

1. Decoder 2 at the Relay: Define

$$i_{UZ|S}(\boldsymbol{u};\boldsymbol{z}|\boldsymbol{s}) \triangleq \log \frac{p_{UZ|S}(\boldsymbol{u},\boldsymbol{z}|\boldsymbol{s})}{p_{U|S}(\boldsymbol{u}|\boldsymbol{s})p_{Z|S}(\boldsymbol{z}|\boldsymbol{s})},$$

$$\mathcal{A}_{UZ|S,\epsilon} \triangleq \{(\boldsymbol{s},\boldsymbol{u},\boldsymbol{z}) \in \mathcal{S}^n \times \mathcal{U}^n \times \mathcal{Z}^n : \tfrac{1}{n} i_{UZ|S}(\boldsymbol{u};\boldsymbol{z}|\boldsymbol{s}) > R_0 + \epsilon\}.$$

The relay declares that the message $\hat{t}_i$ is sent if there is a unique $\hat{t}_i$ such that

$$\big(\boldsymbol{s}(w_i), \boldsymbol{u}(w_i,\hat{t}_i), \boldsymbol{z}_i\big) \in \mathcal{A}_{UZ|S,\epsilon}.$$

It will be shown that the decoding error in this step is small for sufficiently large n if $R_0 < I(U;Z|S)$.

2. Decoders 1a and 1b at the Receiver: Define

$$i_{SY}(\boldsymbol{s};\boldsymbol{y}) \triangleq \log \frac{p_{SY}(\boldsymbol{s},\boldsymbol{y})}{p_S(\boldsymbol{s})p_Y(\boldsymbol{y})},$$

$$i_{UY|S}(\boldsymbol{u};\boldsymbol{y}|\boldsymbol{s}) \triangleq \log \frac{p_{UY|S}(\boldsymbol{u},\boldsymbol{y}|\boldsymbol{s})}{p_{U|S}(\boldsymbol{u}|\boldsymbol{s})p_{Y|S}(\boldsymbol{y}|\boldsymbol{s})},$$

$$\mathcal{A}_{SY,\epsilon} \triangleq \{(\boldsymbol{s},\boldsymbol{y}) \in \mathcal{S}^n \times \mathcal{Y}^n : \tfrac{1}{n}\log i_{SY}(\boldsymbol{s};\boldsymbol{y}) > r + \epsilon\},$$

$$\mathcal{A}_{UY|S,\epsilon} \triangleq \{(\boldsymbol{s},\boldsymbol{u},\boldsymbol{y}) \in \mathcal{S}^n \times \mathcal{U}^n \times \mathcal{Y}^n : \tfrac{1}{n} i_{UY|S}(\boldsymbol{u};\boldsymbol{y}|\boldsymbol{s}) + r > R_0 + \epsilon\}.$$

The receiver first declares that the message $\hat{w}_i$ is sent if there is a unique $\hat{w}_i$ such that $(\boldsymbol{s}(\hat{w}_i), \boldsymbol{y}_i) \in \mathcal{A}_{SY,\epsilon}$. It will be shown that the decoding error in this step is small for sufficiently large n if $r < I(Y;S)$. Next, the receiver, having known w_{i-1} and $\hat{w}_i$, declares that the message $\hat{\hat{t}}_{i-1}$ is sent if there is a unique $\hat{\hat{t}}_{i-1}$ such that

$$\Big(\boldsymbol{s}(w_{i-1}), \boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}), \boldsymbol{y}_{i-1}\Big) \in \mathcal{A}_{UY|S,\epsilon}$$
$$\text{and } \hat{\hat{t}}_{i-1} \in \mathcal{T}_n(\hat{w}_i).$$

It will be shown that the decoding error in this step is small for sufficiently large n if

$$\begin{aligned} R_0 &< I(U;Y|S) + r \\ &< I(U;Y|S) + I(Y;S) = I(US;Y). \end{aligned}$$

3. Decoder 1c at the Receiver: Define

$$i_{XY|US}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{u},\boldsymbol{s}) \triangleq \log \frac{p_{XY|US}(\boldsymbol{x},\boldsymbol{y}|\boldsymbol{u},\boldsymbol{s})}{p_{X|US}(\boldsymbol{x}|\boldsymbol{u},\boldsymbol{s})p_{Y|US}(\boldsymbol{y}|\boldsymbol{u},\boldsymbol{s})},$$

$$\mathcal{A}_{XY|US,\epsilon} \triangleq \{(\boldsymbol{s},\boldsymbol{u},\boldsymbol{x},\boldsymbol{y}) \in \mathcal{S}^n \times \mathcal{U}^n \times \mathcal{X}^n \times \mathcal{Y}^n : \tfrac{1}{n} i_{XY|US}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{u},\boldsymbol{s}) > r_1 + r_2 + \epsilon\}.$$

The receiver, having known w_{i-1}, $\hat{\hat{t}}_{i-1}$, declares that the message pair $(\hat{j}_{i-1}, \hat{l}_{i-1})$ is sent if there is a unique pair $(\hat{j}_{i-1}, \hat{l}_{i-1})$ such that

$$\Big(\boldsymbol{s}(w_{i-1}), \boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}), \boldsymbol{x}(w_{i-1},\hat{\hat{t}}_{i-1},\hat{j}_{i-1},\hat{l}_{i-1}), \boldsymbol{y}_{i-1}\Big) \in \mathcal{A}_{XY|US,\epsilon}.$$

It will be shown that the decoding error in this step is small for sufficiently large n if $r_1 + r_2 < I(X;Y|US)$.

For convenience we show the encoding and decoding processes at the blocks $i-1$, i,, and $i+1$ in Fig. 6.

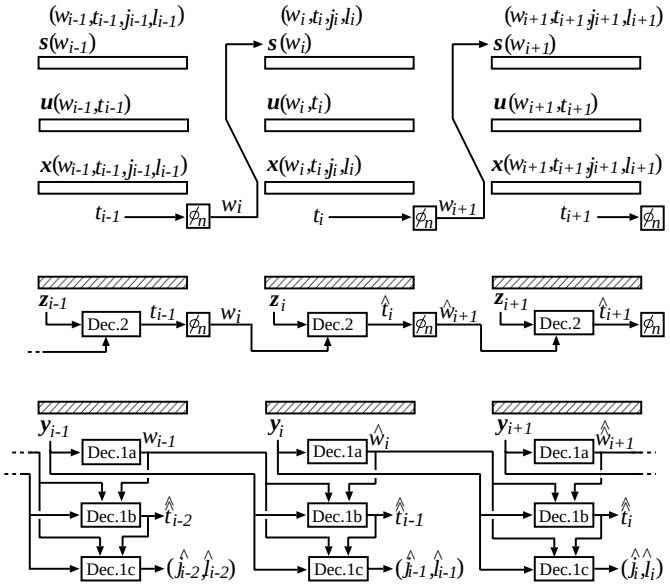

Fig. 6. Encoding and decoding processes at the blocks $i-1$, i, and $i+1$.

B. Computation of Error Probability and Equivocation Rate

In this subsection we compute error probabilities of decoding and equivocation rate for the encoding and decoding scheme stated in the previous subsection. We will declare an error in block i if one or more of the following events occurs.

$\mathcal{E}_{2,i}$: Decoder 2 fails. Let $\mathcal{E}_{2,i} = \tilde{\mathcal{E}}_{2,i} \cup \hat{\mathcal{E}}_{2,i}$, where
$\tilde{\mathcal{E}}_{2,i}$: $(\boldsymbol{s}(w_i), \boldsymbol{u}(w_i,t_i), \boldsymbol{z}_i) \notin \mathcal{A}_{UZ|S,\epsilon}$,
$\hat{\mathcal{E}}_{2,i}$: $\exists\ \hat{t}_i \neq t_i$ such that $(\boldsymbol{s}(w_i),\ \boldsymbol{u}(w_i,\hat{t}_i),\ \boldsymbol{z}_i) \in \mathcal{A}_{UZ|S,\epsilon}$.

$\mathcal{E}_{1a,i}$: Decoder 1a fails. Let $\mathcal{E}_{1a,i} = \tilde{\mathcal{E}}_{1a,i} \cup \hat{\mathcal{E}}_{1a,i}$, where
$\tilde{\mathcal{E}}_{1a,i}$: $(\boldsymbol{s}(w_i), \boldsymbol{y}_i) \notin \mathcal{A}_{SY,\epsilon}$,
$\hat{\mathcal{E}}_{1a,i}$: $\exists\ \hat{w}_i \neq w_i$ such that $(\boldsymbol{s}(w_i),\ \boldsymbol{y}_i) \in \mathcal{A}_{SY,\epsilon}$.

$\mathcal{E}_{1b,i}$: Decoder 1b fails. Let $\mathcal{E}_{1b,i} = \tilde{\mathcal{E}}_{1b,i} \cup \hat{\mathcal{E}}_{1b,i}$, where
$\tilde{\mathcal{E}}_{1b,i}$: $(\boldsymbol{s}(w_{i-1}),\ \boldsymbol{u}(w_{i-1},t_{i-1}),\ \boldsymbol{y}_{i-1}) \notin \mathcal{A}_{UY|S,\epsilon}$,
$\hat{\mathcal{E}}_{1b,i}$: $\exists\ \hat{\hat{t}}_{i-1} \neq t_{i-1}$ such that $(\boldsymbol{s}(w_{i-1}),\ \boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\ \boldsymbol{y}_{i-1}) \in \mathcal{A}_{UY|S,\epsilon}$, $\hat{\hat{t}}_{i-1} \in \mathcal{T}_n(w_i)$.

$\mathcal{E}_{1c,i}$: Decoder 1c fails. Let $\mathcal{E}_{1c,i} = \tilde{\mathcal{E}}_{1c,i} \cup \hat{\mathcal{E}}_{1c,i}$, where
$\tilde{\mathcal{E}}_{1c,i}$: $(\boldsymbol{s}(w_{i-1}),\ \boldsymbol{u}(w_{i-1},\ t_{i-1}),\ \boldsymbol{x}_{i-1}(w_{i-1},\ t_{i-1}, j_{i-1},\ l_{i-1}),\ \boldsymbol{y}_{i-1}) \notin \mathcal{A}_{XY|US,\epsilon}$,
$\hat{\mathcal{E}}_{1c,i}$: $\exists\ (\hat{j}_{i-1},\hat{l}_{i-1}) \neq (j_{i-1},l_{i-1})$ such that $(\boldsymbol{s}(w_{i-1}),\ \boldsymbol{u}(w_{i-1},\ t_{i-1}),\ \boldsymbol{x}_{i-1}(w_{i-1},\ t_{i-1},\ \hat{j}_{i-1},\ \hat{l}_{i-1}),\ \boldsymbol{y}_{i-1}) \in \mathcal{A}_{XY|US,\epsilon}$.

For each $i = 1, 2, \cdots, B$, let $(T_{n,i}, J_{n,i}, L_{n,i}) \in \mathcal{T}_n \times \mathcal{J}_n \times \mathcal{L}_n$ be a message triple to be transmitted at the block i. We

assume that $(T_{n,i}, J_{n,i}, L_{n,i})$, $i = 1, 2, \cdots, B$ are i.i.d. random triples uniformly distributed on $\mathcal{T}_n \times \mathcal{J}_n \times \mathcal{L}_n$. For $i = 0$, $T_{n,0}$, $J_{n,0}$ and $L_{n,0}$ are constant. For $i = 1, 2, \cdots, B-1$, define the random variable $W_{n,i}$ on $\mathcal{W}_n$ by $W_{n,i} = \phi_n(T_{n,i-1})$. Define the error events $\mathcal{F}_i$ for decoding errors in block i by

$\mathcal{F}_i$: $\hat{W}_{n,i} \neq W_{n,i}$ or $\hat{T}_{n,i} \neq T_{n,i}$ or $\hat{\hat{T}}_{n,i-1} \neq T_{n,i-1}$ or $(\hat{J}_{n,i-1}, \hat{L}_{n,i-1}) \neq (J_{n,i-1}, L_{n,i-1})$.

It is obvious that $\mathcal{F}_i \subseteq \mathcal{E}_{2,i} \cup \mathcal{E}_{1\mathrm{a},i} \cup \mathcal{E}_{1\mathrm{b},i} \cup \mathcal{E}_{1\mathrm{c},i}$. Define $e_{2,i}^{(n)} \stackrel{\triangle}{=} \Pr\left\{\mathcal{E}_{2,i} | \mathcal{F}_{i-1}^c\right\}$. Definitions of $e_{1\mathrm{a},i}^{(n)}$, $e_{1\mathrm{b},i}^{(n)}$, and $e_{1\mathrm{c},i}^{(n)}$ are the same as that of $e_{2,i}^{(n)}$. We further define sets and quantities necessary for computation of the equivocation rate. Define

$$i_{XZ|US}(\boldsymbol{x}; \boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s}) \stackrel{\triangle}{=} \log \frac{p_{XZ|US}(\boldsymbol{x}, \boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s})}{p_{X|US}(\boldsymbol{x}|\boldsymbol{u}, \boldsymbol{s}) p_{Z|US}(\boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s})},$$

$$\mathcal{A}_{XZ|US,\epsilon} \stackrel{\triangle}{=} \{(\boldsymbol{s}, \boldsymbol{u}, \boldsymbol{x}, \boldsymbol{y}) \in \mathcal{S}^n \times \mathcal{U}^n \times \mathcal{X}^n \times \mathcal{Z}^n : \frac{1}{n} i_{XZ|US}(\boldsymbol{x}; \boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s}) > r_2 + \epsilon\}.$$

For given $w_i = \psi_n(t_{i-1}) \in \mathcal{W}_n$, $(t_i, l_i) \in \mathcal{T}_n \times \mathcal{L}_n$ and channel output $\boldsymbol{z}_i$ of $\boldsymbol{s}(w_i)$ and $\boldsymbol{x}(w_i, t_i, j_i, l_i)$, define the estimation function $\tau_n : \mathcal{W}_n \times \mathcal{T}_n \times \mathcal{L}_n \times \mathcal{Z}^n \to \mathcal{J}_n$ by $\tau_n(w_i, t_i, l_i, \boldsymbol{z}_i) = \hat{j}_i$ if there is a unique pair $(\hat{j}_i, l_i)$ such that

$$\left(\boldsymbol{s}(w_i), \boldsymbol{u}(w_i, t_i), \boldsymbol{x}(w_i, t_i, \hat{j}_i, l_i), \boldsymbol{z}_i\right) \in \mathcal{A}_{XZ|US,\epsilon}.$$

Define $e_i^{(n)} \stackrel{\triangle}{=} \Pr\{\tau_n(W_{n,i}, T_{n,i}, L_{n,i}, Z^n) \neq J_{n,i}\}$. Let

$\tilde{\mathcal{E}}_i$: $(\boldsymbol{s}(w_{i-1}), \boldsymbol{u}(w_{i-1}, t_{i-1}), \boldsymbol{x}_{i-1}(w_{i-1}, t_{i-1}, j_{i-1}, l_{i-1}), \boldsymbol{z}_{i-1}) \notin \mathcal{A}_{XZ|US,\epsilon}$,

$\hat{\mathcal{E}}_i$: $\exists\ \hat{j}_{i-1} \neq j_{i-1}$ such that $(\boldsymbol{s}(\ w_{i-1}),\ \boldsymbol{u}(w_{i-1},\ t_{i-1}),\ \boldsymbol{x}_{i-1}(w_{i-1},\ t_{i-1},\ \hat{j}_{i-1},\ l_{i-1}),\ \boldsymbol{z}_{i-1}) \in \mathcal{A}_{XZ|US,\epsilon}$.

Set $\mathcal{E}_i = \tilde{\mathcal{E}}_i \cup \hat{\mathcal{E}}_i$. Then we have

$$e_i^{(n)} = \Pr\{\mathcal{E}_i\} \leq \Pr\{\tilde{\mathcal{E}}_i\} + \Pr\{\hat{\mathcal{E}}_i\}.$$

It will be shown that the error probability $e_i^{(n)}$ of estimation is small for sufficiently large n if $r_2 < I(X; Z|US)$. Set

$$i_{Z|XS}(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{s}) \stackrel{\triangle}{=} -\log p_{Z|XS}(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{s}),$$

$$i_{Z|US}(\boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s}) \stackrel{\triangle}{=} -\log p_{Z|US}(\boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s}),$$

$$\mathcal{B}_{Z|XS,\epsilon} \stackrel{\triangle}{=} \left\{(\boldsymbol{s}, \boldsymbol{x}, \boldsymbol{z}) \in \mathcal{S}^n \times \mathcal{X}^n \times \mathcal{Z}^n : \frac{1}{n} i_{Z|XS}(\boldsymbol{z}|\boldsymbol{x}, \boldsymbol{s}) \geq H(Z|XS) - \epsilon\right\},$$

$$\mathcal{B}_{Z|US,\epsilon} \stackrel{\triangle}{=} \left\{(\boldsymbol{s}, \boldsymbol{u}, \boldsymbol{z}) \in \mathcal{S}^n \times \mathcal{U}^n \times \mathcal{Z}^n : \frac{1}{n} i_{Z|US}(\boldsymbol{z}|\boldsymbol{u}, \boldsymbol{s}) \leq H(Z|US) + \epsilon\right\},$$

$$e_{Z|XS,i}^{(n)} \stackrel{\triangle}{=} \Pr\{\boldsymbol{s}(W_{n,i}), \boldsymbol{x}(W_{n,i}, T_{n,i}, L_{n,i}), Z_i^n) \notin \mathcal{B}_{Z|XS,\epsilon}\},$$

$$e_{Z|US,i}^{(n)} \stackrel{\triangle}{=} \Pr\{(\boldsymbol{s}(W_{n,i}), \boldsymbol{u}(T_{n,i}), Z_i^n) \notin \mathcal{B}_{Z|US,\epsilon}\}.$$

The operation $\mathsf{E}\left[e_{2,i}^{(n)}\right]$ stands for the expectation of $e_{2,i}^{(n)}$ based on the randomness of code construction. Then, we have the following lemma.

Lemma 2: For each $i = 1, 2, \cdots, B-1$, we have

$$\mathsf{E}\left[e_{2,i}^{(n)}\right] \leq \Pr\{(S^n, U^n, Z^n) \notin \mathcal{A}_{UZ|S,\epsilon}\} + 2^{-n\epsilon}$$

$$\mathsf{E}\left[e_{1\mathrm{a},i}^{(n)}\right] \leq \Pr\{(S^n, Y^n) \notin \mathcal{A}_{SY,\epsilon}\} + 2^{-n\epsilon}$$

$$\mathsf{E}\left[e_{1\mathrm{b},i}^{(n)}\right] \leq \Pr\{(S^n, U^n, Y^n) \notin \mathcal{A}_{UY|S,\epsilon}\} + 2 \cdot 2^{-n\epsilon}$$

$$\mathsf{E}\left[e_{1\mathrm{c},i}^{(n)}\right] \leq \Pr\{(S^n, U^n, X^n, Y^n) \notin \mathcal{A}_{XY|SU,\epsilon}\} + 2^{-n\epsilon}$$

$$\mathsf{E}\left[e_i^{(n)}\right] \leq \Pr\{(S^n, U^n, X^n, Z^n) \notin \mathcal{A}_{XZ|SU,\epsilon}\} + 2^{-n\epsilon}$$

$$\mathsf{E}\left[e_{Z|XS,i}^{(n)}\right] = \Pr\{(S^n, X^n, Z^n) \notin \mathcal{B}_{Z|XS,\epsilon}\}$$

$$\mathsf{E}\left[e_{Z|US,i}^{(n)}\right] = \Pr\{(S^n, U^n, Z^n) \notin \mathcal{B}_{Z|US,\epsilon}\}.$$

Proof of this lemma is given in Appendix A.

Next, we state a key lemma useful for the computation of the equivocation rate. Set $L_n^{(i)} \stackrel{\triangle}{=} (L_{n,1}, L_{n,2}, \cdots, L_{n,i})$. Then, the equivocation rate over B blocks is

$$\frac{1}{nB} H(L_n^{(B)}|Z^{nB}) \geq \frac{1}{B} \sum_{i=1}^{B-1} \frac{1}{n} H(L_{n,i}|L_n^{(i-1)} Z^{nB}).$$

For each $i = 1, 2, \cdots, B-1$, we estimate a lower bound of $H(L_{n,i}|\ L_n^{(i-1)} Z^{nB})$. Set $Z_{n(i-1)+1}^{ni} \stackrel{\triangle}{=} (Z_{n(i-1)+1}, \cdots, Z_{ni})$. On a lower bound of $H(L_{n,i}|L_n^{(i-1)} Z^{nB})$, we have the following lemma.

Lemma 3: For $i = 1, 2, \cdots, B-1$, we have

$$\begin{aligned} &\frac{1}{n} H(L_{n,i}|L_n^{(i-1)} Z^{nB}) \\ &\geq r_1 + r_2 - I(X; Z|US) - 2\epsilon - \frac{3 + \log \mathrm{e}}{n} \\ &\quad - r_2 e_i^{(n)} - (\log |\mathcal{Z}|) \left[e_{Z|US,i}^{(n)} + e_{Z|XS,i}^{(n)}\right]. \end{aligned} \tag{11}$$

Proof of this lemma is given in Appendix B.

Proof of Lemma 1: Set

$$\begin{aligned} &\gamma_{\max}(\epsilon) \\ &\stackrel{\triangle}{=} \max\{\ \Pr\{(S^n, U^n, Z^n) \notin \mathcal{A}_{UZ|S,\epsilon}\} + 2^{-n\epsilon}, \\ &\qquad \Pr\{(S^n, Y^n) \notin \mathcal{A}_{SY,\epsilon}\} + 2^{-n\epsilon}, \\ &\qquad \Pr\{(S^n, U^n, Y^n) \notin \mathcal{A}_{UY|S,\epsilon}\} + 2^{-n\epsilon}, \\ &\qquad \Pr\{(S^n, U^n, X^n, Y^n) \notin \mathcal{A}_{XY|SU,\epsilon}\} + 2^{-n\epsilon}, \\ &\qquad \Pr\{(S^n, U^n, X^n, Z^n) \notin \mathcal{A}_{XZ|SU,\epsilon}\} + 2^{-n\epsilon}, \\ &\qquad \Pr\{(S^n, X^n, Z^n) \notin \mathcal{B}_{Z|XS,\epsilon}\}, \\ &\qquad \Pr\{(S^n, U^n, Z^n) \notin \mathcal{B}_{Z|US,\epsilon}\}\ \}. \end{aligned}$$

Then, by Lemma 2, we obtain

$$\begin{aligned} &\mathsf{E}\left[\sum_{i=1}^{B-1} \left\{e_{2,i}^{(n)} + e_{1\mathrm{a},i}^{(n)} + e_{1\mathrm{b},i}^{(n)} + e_{1\mathrm{c},i}^{(n)} + e_i^{(n)} + e_{Z|XS,i}^{(n)} + e_{Z|US,i}^{(n)}\right\}\right] \\ &= \sum_{i=1}^{B-1} \left\{\mathsf{E}\left[e_{2,i}^{(n)}\right] + \mathsf{E}\left[e_{1\mathrm{a},i}^{(n)}\right] + \mathsf{E}\left[e_{1\mathrm{b},i}^{(n)}\right] + \mathsf{E}\left[e_{1\mathrm{c},i}^{(n)}\right] + \mathsf{E}\left[e_i^{(n)}\right] + \mathsf{E}\left[e_{Z|XS,i}^{(n)}\right] + \mathsf{E}\left[e_{Z|US,i}^{(n)}\right]\right\} \\ &\leq 7(B-1)\gamma_{\max}(\epsilon), \end{aligned}$$

from which it follows that there exist at least one deterministic code such that

$$\sum_{i=1}^{B-1}\Big\{e_{2,i}^{(n)}+e_{1\mathrm{a},i}^{(n)}+e_{1\mathrm{b},i}^{(n)}+e_{1\mathrm{c},i}^{(n)}+e_{i}^{(n)} +e_{Z|XS,i}^{(n)}+e_{Z|US,i}^{(n)}\Big\}\le 7(B-1)\gamma_{\max}^{(n)}(\epsilon)\,. \quad (12)$$

From (12), we have

$$\mu_1^{(nB)}=\sum_{i=1}^{B-1}\Big\{e_{1\mathrm{a},i}^{(n)}+e_{1\mathrm{b},i}^{(n)}+e_{1\mathrm{c},i}^{(n)}\Big\} \le 7(B-1)\gamma_{\max}^{(n)}(\epsilon)\,, \quad (13)$$

$$\mu_2^{(nB)}=\sum_{i=1}^{B-1}e_{2,i}^{(n)}\le 7(B-1)\gamma_{\max}^{(n)}(\epsilon)\,, \quad (14)$$

$$\sum_{i=1}^{B-1}e_{i}^{(n)}\le 7(B-1)\gamma_{\max}^{(n)}(\epsilon)\,, \quad (15)$$

$$\sum_{i=1}^{B-1}\Big\{e_{Z|XS,i}^{(n)}+e_{Z|US,i}^{(n)}\Big\}\le 7(B-1)\gamma_{\max}^{(n)}(\epsilon)\,. \quad (16)$$

From Lemma 3, (15), and (16), we have

$$\begin{aligned}&\frac{1}{nB}H(L_n^{(B)}|Z^{nB})\\ &\ge\frac{1}{B}\sum_{i=1}^{B-1}\frac{1}{n}H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\ &\ge\left(1-\frac{1}{B}\right)\left[r_1+r_2-I(X;Z|US)-2\epsilon-\frac{3+\log\mathrm{e}}{n}\right]\\ &\quad-7\left(1-\frac{1}{B}\right)[r_2+(\log|\mathcal{Z}|)]\gamma_{\max}^{(n)}(\epsilon)\,. \end{aligned}\quad (17)$$

By the weak law of large numbers, when $n\to\infty$, we have

$$\left.\begin{array}{l}\frac{1}{n}i_{UZ|S}(U^n;Z^n|S^n)\to I(U;Z|S)\\ \frac{1}{n}i_{SY}(S^n;Y^n)\to I(S;Y)\\ \frac{1}{n}i_{UY|S}(U^n;Y^n|S^n)\to I(U;Y|S)\\ \frac{1}{n}i_{XY|US}(X^n;Y^n|U^nS^n)\to I(X;Y|US)\\ \frac{1}{n}i_{XZ|US}(X^n;Z^n|U^nS^n)\to I(X;Z|US)\\ \frac{1}{n}i_{Z|XS}(Z^n|X^nS^n)\to H(Z|XS)\\ \frac{1}{n}i_{Z|US}(Z^n|U^nS^n)\to H(Z|US)\end{array}\right\} \quad (18)$$

in probability. Fix $\epsilon>0$ arbitrary and choose

$$\left.\begin{array}{l}R_0=\min\{I(U;Z|S),I(U;Y|S)+r\}-2\epsilon\\ r=I(S;Y)-2\epsilon\\ r_1=I(X;Y|US)-I(X;Z|US)-2\epsilon\\ r_2=I(X;Z|US)-\epsilon\,.\end{array}\right\} \quad (19)$$

Then, it follows from (18) and the definition of $\gamma_{\max}^{(n)}(\epsilon)$ that for the choice of (R_0,r,r_1,r_2) in (19), we have

$$\lim_{n\to\infty}\gamma_{\max}^{(n)}(\epsilon)=0\,. \quad (20)$$

For $n=1,2,\cdots$, we choose block $B=B_n$ so that $B_n=\left\lfloor\left(\gamma_{\max}^{(n)}(\epsilon)\}\right)^{-1/2}\right\rfloor$. Define $\{g_i\}_{i=1}^{nB_n}$ by

$$g_i\triangleq\begin{cases}\phi_n, & \text{if } i \bmod n=0\,,\\ \text{constant}, & \text{otherwise}\,.\end{cases}$$

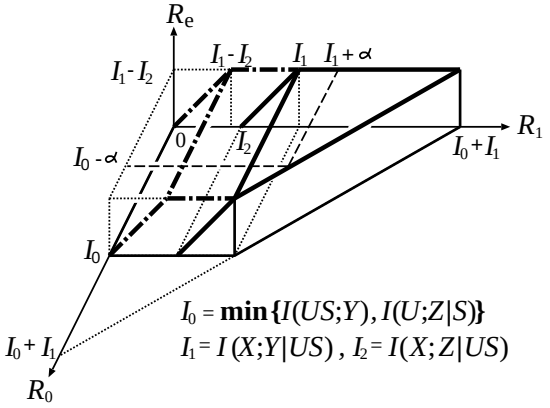

Fig. 7. Shapes of $\check{\mathcal{R}}_{\mathrm{s}}^{(\mathrm{in})}(U,X,S|\Gamma)$ and $\mathcal{R}_{\mathrm{d}}^{(\mathrm{in})}(U,X,S|\Gamma)$.

Define the sequence of block codes $\{(f_\nu,\ \{g_i\}_{i=1}^{\nu},\ \psi_\nu,\ \varphi_\nu)\}_{\nu=1}^{\infty}$ by

$$(f_\nu,\{g_i\}_{i=1}^{\nu},\psi_\nu,\varphi_\nu)\triangleq\begin{cases}\text{constant, if } 1\le\nu<B_1\,,\\ (f_{nB_n},\{g_i\}_{i=1}^{nB_n},\psi_{nB_n},\varphi_{nB_n})\,,\\ \text{if } nB_n\le\nu<(n+1)B_{n+1}\,.\end{cases}$$

Combining (13), (14), (17), and (20), we have that there exists a sequence of block codes $\{(f_\nu,\ \{g_i\}_{i=1}^{\nu},\ \psi_\nu,\ \varphi_\nu)\}_{\nu=1}^{\infty}$ such that

$$\begin{aligned}&\lim_{\nu\to\infty}\mu_1^{(\nu)}=\lim_{n\to\infty}\mu_1^{(nB_n)}\le\lim_{n\to\infty}7\sqrt{\gamma_{\max}^{(n)}(\epsilon)}=0\,,\\ &\lim_{\nu\to\infty}\mu_2^{(\nu)}=\lim_{n\to\infty}\mu_2^{(nB_n)}\le\lim_{n\to\infty}7\sqrt{\gamma_{\max}^{(n)}(\epsilon)}=0\,,\\ &\lim_{\nu\to\infty}\frac{1}{\nu}\log|\mathcal{T}_\nu|=\lim_{n\to\infty}\frac{1}{nB_n}\log|(\mathcal{T}_n)^{B_n-1}|\\ &=R_0=\min\{I(U;Z|S),I(US;Y)-2\epsilon\}-2\epsilon\,,\\ &\lim_{\nu\to\infty}\frac{1}{\nu}\log|\mathcal{J}_\nu|=\lim_{n\to\infty}\frac{1}{nB_n}\log|(\mathcal{J}_n)^{B_n-1}|\\ &=r_2=I(X;Z|US)-\epsilon\,,\\ &\lim_{\nu\to\infty}\frac{1}{\nu}\log|\mathcal{L}_\nu|=\lim_{n\to\infty}\frac{1}{nB_n}\log|(\mathcal{L}_n)^{B_n-1}|\\ &=r_1=I(X;Y|US)-I(X;Z|US)-2\epsilon\,,\\ &\lim_{\nu\to\infty}\frac{1}{\nu}H(L_\nu|Z^\nu)=\lim_{n\to\infty}\frac{1}{nB_n}H(L_n^{(B_n)}|Z^{nB_n})\\ &\ge I(X;Y|US)-I(X;Z|US)-5\epsilon\,.\end{aligned}$$

Since ϵ can be arbitrary small, we obtain the desired result for the above sequence of block codes. Thus, the proof of Lemma 1 is completed. ■

C. Proofs of the Direct Coding Theorems

In this subsection we prove $\mathcal{R}_{\mathrm{d}}^{(\mathrm{in})}(\Gamma)$,$\tilde{\mathcal{R}}_{\mathrm{d}}^{(\mathrm{in})}(\Gamma)\subseteq\mathcal{R}_{\mathrm{d}}(\Gamma)$ and $\mathcal{R}_{\mathrm{s}}^{(\mathrm{in})}(\Gamma)\subseteq\mathcal{R}_{\mathrm{s}}(\Gamma)$. Set

$$\begin{aligned}&\check{\mathcal{R}}_{\mathrm{s}}^{(\mathrm{in})}(U,X,S|\Gamma)\\ &\triangleq\{(R_0,R_1,R_{\mathrm{e}}):R_0,R_1,R_{\mathrm{e}}\ge0\,,\\ &\quad R_0\le\min\{I(US;Y),I(U;Z|S)\}\,,\\ &\quad R_0+R_1\le I(X;Y|US)\\ &\qquad+\min\{I(U;Z|S),I(US;Y)\}\,,\\ &\quad R_{\mathrm{e}}\le R_1\,,\\ &\quad R_{\mathrm{e}}\le[I(X;Y|US)-I(X;Z|US)]^+.\}\,,\end{aligned}$$

and

$$\check{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma) \stackrel{\triangle}{=} \bigcup_{(U,X,S)\in\mathcal{P}_1} \check{\mathcal{R}}_{\rm s}^{(\rm in)}(U,X,S|\Gamma)\,.$$

Proof of $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma)$ *and* $\check{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm s}(\Gamma)$ *:* Set

$$I_0 \stackrel{\triangle}{=} \min\{I(US;Y), I(U;Z|S)\}\,,$$
$$I_1 \stackrel{\triangle}{=} I(X;Y|US), I_2 \stackrel{\triangle}{=} I(X;Z|US)\,.$$

We consider the case that $I_1 \geq I_2$. The region $\check{\mathcal{R}}(U,X,S|\Gamma)$ in this case is depicted in Fig. 7. We first prove $\mathcal{R}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma)$. From the shape of the region $\mathcal{R}_{\rm d}^{(\rm in)}(U,X,S|\Gamma)$, it suffices to show that for every

$$\alpha \in [0, \min\{I(US;Y), I(U;Z|S)\}],$$

the following $(R_0, R_1, R_{\rm e})$ is achievable:

$$R_0 = \min\{I(US;Y), I(U;Z|S)\} - \alpha\,,$$
$$R_1 = I(X;Y|US) + \alpha\,,$$
$$R_{\rm e} = I(X;Y|US) - I(X;Z|US)\,.$$

Choose $\mathcal{T}_n'$ and $\mathcal{T}_n''$ such that

$$\mathcal{T}_n = \mathcal{T}_n' \times \mathcal{T}_n''\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{T}_n'| = \min\{I(US;Y), I(U;Z|S)\} - \alpha\,.$$

We take

$$\mathcal{M}_n = \mathcal{T}_n'\,, \quad \mathcal{K}_n = \mathcal{T}_n'' \times \mathcal{J}_n \times \mathcal{L}_n\,.$$

Then, by Lemma 1, we have

$$\lim_{n\to\infty}\mu_1^{(n)} = \lim_{n\to\infty}\mu_2^{(n)} = 0,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{K}_n| = I(X;Y|US) + \alpha\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{M}_n| = \min\{I(US;Y), I(U;Z|S)\} - \alpha\,,$$
$$\lim_{n\to\infty}\frac{1}{n}H(K_n|Z^n) \geq \lim_{n\to\infty}\frac{1}{n}H(L_n|Z^n) \geq I(X;Y|US) - I(X;Z|US)\,.$$

To help understating the above proof, information quantities contained in the transmitted messages are shown in Fig. 8. Next we prove $\check{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm s}(\Gamma)$. From the shape of the region $\check{\mathcal{R}}_{\rm s}^{(\rm in)}(U,X,S|\Gamma)$, it suffices to show that the following $(R_0, R_1, R_{\rm e})$ is achievable:

$$R_0 = \min\{I(US;Y), I(U;Z|S)\}\,,$$
$$R_1 = R_{\rm e} = I(X;Y|US) - I(X;Z|US)\,.$$

Choose $f_n : \mathcal{T}_n \times \mathcal{J}_n \times \mathcal{L}_n \to \mathcal{X}^n$ specified in Lemma 1. Set $\mathcal{M}_n = \mathcal{T}_n$ and $\mathcal{K}_n = \mathcal{L}_n$. Using this f_n, for $(m,k) \in \mathcal{M}_n \times \mathcal{K}_n$ define

$$f_n(m, J_n, k) = \boldsymbol{x}(m, J_n, k) \in \mathcal{X}^n\,.$$

The above f_n is no longer a deterministic function. It becomes a random function randomized by J_n uniformly distributed on

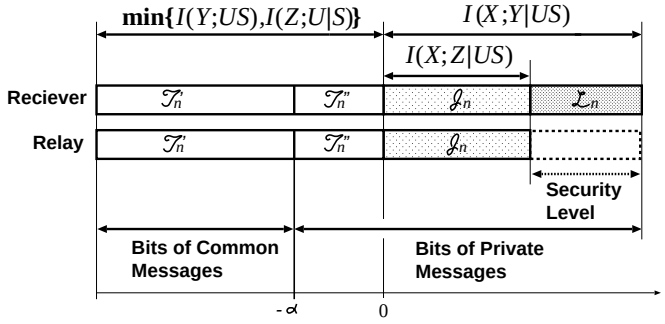

Fig. 8. Information contained in the transmitted messages.

$\mathcal{J}_n$, which works as a "dummy" random variable. It is obvious that this random function attains

$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{M}_n| = \min\{I(US;Y), I(U;Z|S)\}\,,$$
$$\lim_{n\to\infty}\frac{1}{n}\log|\mathcal{K}_n| = I(X;Y|US) - I(X;Z|US)\,,$$
$$\lim_{n\to\infty}\frac{1}{n}H(K_n|Z^n) \geq I(X;Y|US) - I(X;Z|US)\,,$$

completing the proof. ■

Proof of $\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma)$*:* Since $\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}^{(\rm in)}(\Gamma)$, we have $\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm d}(\Gamma)$. ■

Proof of $\mathcal{R}_{\rm s}^{(\rm in)}(\Gamma) \subseteq \mathcal{R}_{\rm s}(\Gamma)$*:* Choose $(U,V,X,S) \in \mathcal{Q}_1$. The joint distribution of (U,V,X,S) is given by

$$p_{UVXS}(u,v,x,s) = p_{USV}(u,s,v)p_{X|V}(x|v)\,,\ (u,v,x,s) \in \mathcal{U}\times\mathcal{V}\times\mathcal{X}\times\mathcal{S}\,.$$

Consider the discrete memoryless channels with input alphabet $\mathcal{V}\times\mathcal{S}$ and output alphabet $\mathcal{Y}\times\mathcal{Z}$, and stochastic matrices defined by the conditional distribution of (Y,Z) given V,S having the form

$$\Gamma'(y,z|v,s) = \sum_{x\in\mathcal{X}}\Gamma(y,z|x,s)p_{X|V}(x|v)\,.$$

Any encoder $f_n' : \mathcal{K}_n \times \mathcal{M}_n \to \mathcal{V}^n$ for this new RCC determines a *stochastic* encoder f_n for the original RCC by the matrix product of f_n' with the stochastic matrix given by $p_{X|V} = \{p_{X|V}(x|v)\}_{(v,x)\in\mathcal{V}\times\mathcal{X}}$. Both encoders yield the same stochastic connection of messages and received sequences, so the assertion follows by choosing the encoder f_n' used for the proof of the inclusion $\check{\mathcal{R}}_{\rm s}^{(\rm in)}(\Gamma') \subseteq \mathcal{R}_{\rm s}(\Gamma')$. ■

Cardinality bounds of auxiliary random variables in $\mathcal{P}_1$ and $\mathcal{Q}_1$ can be proved by the argument that Csiszár and Körner [5] developed in Appendix in their paper.

VII. Derivations of the Outer Bounds

In this section we derive the outer bounds stated in Theorems 2-5. We further prove Theorem 6. We first remark here that cardinality bounds of auxiliary random variables in $\mathcal{P}_2$ and $\mathcal{Q}_2$ in the outer bounds can be proved by the argument that Csiszár and Körner [5] developed in Appendix in their paper.

The following lemma is a basis on derivations of the outer bounds.

Lemma 4: We assume $(R_0, R_1, R_e) \in \mathcal{R}_s^*(\Gamma)$. Then, we have

$$\left.\begin{aligned} R_0 &\le \tfrac{1}{n}\min\{I(M_n;Y^n), I(M_n;Z^n)\} + \delta_{1,n} \\ R_1 &\le \tfrac{1}{n} I(K_n;Y^n|M_n) + \delta_{2,n} \\ R_e &\le [R_1 - I(K_n;Z^n|M_n)]^+ + \delta_{3,n} \\ R_e &\le \big[\tfrac{1}{n} I(K_n;Y^n|M_n) \\ &\qquad - \tfrac{1}{n} I(K_n;Z^n|M_n)\big]^+ + \delta_{4,n}\,, \end{aligned}\right\} \tag{21}$$

where $\{\delta_{i,n}\}_{n=1}^{\infty}$, $i = 1, 2, 3, 4$ are sequences that tend to zero as $n \to \infty$.

The above lemma can be proved by a standard converse coding argument using Fano's inequality. The detail of the proof is given in Appendix C.

We first prove $\mathcal{R}_d(\Gamma) \subseteq \tilde{\mathcal{R}}_d^{(out)}(\Gamma)$. As a corollary of Lemma 4, we have the following lemma.

Lemma 5: We assume that $(R_0, R_1, R_e) \in \mathcal{R}_s^*(\Gamma)$. Then,

$$\left.\begin{aligned} R_0 &\le \tfrac{1}{n}\min\{I(M_n;Y^n), I(M_n;Z^n)\} + \delta_{1,n} \\ R_1 &\le \tfrac{1}{n} I(K_n;Y^n|M_n) + \delta_{2,n} \\ R_0 + R_1 &\le \tfrac{1}{n} I(K_n M_n;Y^n) + \tilde{\delta}_{3,n} \\ R_e &\le [R_1 - \tfrac{1}{n} I(K_n;Z^n|M_n)]^+ + \delta_{3,n} \\ R_e &\le \big[\tfrac{1}{n} I(K_n;Y^n|M_n) \\ &\qquad - \tfrac{1}{n} I(K_n;Z^n|M_n)\big]^+ + \delta_{4,n}\,, \end{aligned}\right\} \tag{22}$$

where $\tilde{\delta}_3 \triangleq \delta_{1,n} + \delta_{2,n}$.

By this lemma, it suffices to derive upper bounds of

$$I(M_n;Z^n), I(M_n;Y^n), I(K_n;Y^n|M_n),$$
$$I(K_n M_n;Y^n), I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n)$$

to prove $\mathcal{R}_d(\Gamma) \subseteq \tilde{\mathcal{R}}_d^{(out)}(\Gamma)$. For upper bounds of the above five quantities, we have the following Lemma.

Lemma 6: Set

$$U_i \triangleq M_n Y^{i-1} Z^{i-1}\,, \quad i = 1, 2, \cdots, n\,.$$

For $i = 1, 2, \cdots, n$, U_i, $X_i S_i$, and $Y_i Z_i$ form a Markov chain $U_i \to X_i S_i \to Y_i Z_i$ in this order. Furthermore, we have

$$I(M_n;Y^n) \le \sum_{i=1}^{n} I(U_i S_i; Y_i)\,, \tag{23}$$

$$I(M_n;Z^n) \le \sum_{i=1}^{n} I(U_i; Z_i|S_i)\,, \tag{24}$$

$$I(K_n M_n;Y^n) \le \sum_{i=1}^{n} I(X_i S_i; Y_i)\,, \tag{25}$$

$$I(K_n;Y^n|M_n) \le \sum_{i=1}^{n} I(X_i; Y_i Z_i|U_i S_i)\,, \tag{26}$$

$$\begin{aligned} &I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n) \\ &\le \sum_{i=1}^{n} I(X_i;Y_i|Z_i U_i S_i)\,. \end{aligned} \tag{27}$$

The bounds (23)-(26) also hold for any stochastic relay encoder. If Γ belongs to the class NL, the bound (27) also holds for any stochastic relay encoder. If f_n is a deterministic encoder, we have

$$I(K_n;Z^n|M_n) \ge \sum_{i=1}^{n} I(X_i;Z_i|U_i S_i) \tag{28}$$

in addition to (23)-(27). If Γ belongs to the class NL, the bound (28) also holds for any stochastic relay encoder.

Proof of Lemma 6 is given in Appendix D.

Proof of $\mathcal{R}_d(\Gamma) \subseteq \tilde{\mathcal{R}}_d^{(out)}(\Gamma)$ and $\mathcal{R}_s(\Gamma) \subseteq \tilde{\mathcal{R}}_s^{(out)}(\Gamma)$: We first assume that $(R_0, R_1, R_e) \in \mathcal{R}_s(\Gamma)$. Let Q be a random variable independent of $K_n M_n X^n Y^n$ and uniformly distributed on $\{1, 2, \cdots, n\}$. Set

$$X \triangleq X_Q, S \triangleq S_Q, Y \triangleq Y_Q, Z \triangleq Z_Q.$$

Furthermore, set

$$U \triangleq U_Q Q = Z^{Q-1} Y^{Q-1} M_n Q\,.$$

Note that $UXSYZ$ satisfies a Markov chain $U \to XS \to YZ$. By Lemmas 5 and 6, we have

$$\left.\begin{aligned} R_0 &\le \min\{I(US;Y|Q), I(U;Z|SQ)\} + \delta_{1,n} \\ &\le \min\{I(US;Y), I(U;Z|S)\} + \delta_{1,n} \\ R_1 &\le I(X;YZ|US) + \delta_{2,n} \\ R_0 + R_1 &\le I(XS;Y|Q) + \tilde{\delta}_{3,n} \\ &= I(XS;Y) + \tilde{\delta}_{3,n} \\ R_e &\le I(X;Y|ZUS) + \delta_{4,n}\,. \end{aligned}\right\} \tag{29}$$

Using memoryless character of the channel it is straightforward to verify that $U \to XS \to YZ$ and that the conditional distribution of (Y, Z) given XS coincides with the corresponding channel matrix Γ. Hence, by letting $n \to \infty$ in (29), we obtain $(R_0, R_1, R_e) \in \mathcal{R}_s^{(out)}(\Gamma)$. Next we assume that $(R_0, R_1, R_e) \in \mathcal{R}_d(\Gamma)$. Then by Lemmas 5 and 6, we have

$$R_e \le [R_1 - I(X;Z|US)]^+ + \delta_{3,n} \tag{30}$$

in addition to (29). Hence by letting $n \to \infty$ in (29) and (30), we conclude that $(R_0, R_1, R_e) \in \tilde{\mathcal{R}}_d^{(out)}(\Gamma)$. ■

Next we prove the inclusions $\mathcal{R}_d(\Gamma) \subseteq \mathcal{R}_d^{(out)}(\Gamma)$, $\mathcal{R}_d(\Gamma) \subseteq \hat{\mathcal{R}}_d^{(out)}(\Gamma)$, and $\mathcal{R}_s(\Gamma) \subseteq \mathcal{R}_s^{(out)}(\Gamma)$. As a corollary of Lemma 4, we have the following lemma.

Lemma 7: We assume that $(R_0, R_1, R_e) \in \mathcal{R}_s^*(\Gamma)$. Then,

$$\left.\begin{aligned} R_0 &\le \tfrac{1}{n}\min\{I(M_n;Y^n), I(M_n;Z^n)\} + \delta_{1,n} \\ R_0 + R_1 &\le \tfrac{1}{n} I(K_n;Y^n|M_n) \\ &\quad + \tfrac{1}{n}\min\{I(M_n;Y^n), I(M_n;Z^n)\} + \tilde{\delta}_{3,n} \\ R_e &\le [R_1 - \tfrac{1}{n} I(K_n;Z^n|M_n)]^+ + \delta_{3,n} \\ R_e &\le \big[\tfrac{1}{n} I(K_n;Y^n|M_n) \\ &\quad - \tfrac{1}{n} I(K_n;Z^n|M_n)\big]^+ + \delta_{4,n}\,. \end{aligned}\right\} \tag{31}$$

From Lemma 7, it suffices to derive upper bounds of the following five quantities:

$$I(M_n;Z^n), I(M_n;Y^n)\,,$$
$$I(K_n;Y^n|M_n) + I(M_n;Y^n) = I(K_n M_n;Y^n)\,,$$
$$I(K_n;Y^n|M_n) + I(M_n;Z^n)\,, \tag{32}$$
$$I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n)\,. \tag{33}$$

Since

$$\begin{aligned} &I(K_n;Y^n|M_n) + I(M_n;Z^n) \\ &= I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n) + I(K_n M_n;Z^n)\,, \end{aligned}$$

we derive an upper bound of (32) by estimating upper bounds of $I(K_nM_n;Z^n)$ and (33).

The following is a key lemma to prove $\mathcal{R}_{\rm d}(\Gamma)\subseteq\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$.

Lemma 8: Set

$$U_i\stackrel{\triangle}{=}Y_{i+1}^nZ^{i-1}M_n\,,\quad i=1,2,\cdots,n\,,$$

where Y_{i+1}^n stands for $Y_{i+1}Y_{i+2}\cdots Y_n$. For $i=1,2,\cdots,n$, U_i, $X_iS_iZ_i$, and Y_i form a Markov chain $U_i\to X_iZ_iS_i\to Y_i$ in this order. Furthermore, we have

$$I(M_n;Y^n)\le\sum_{i=1}^n I(U_iS_i;Y_i)\,,\tag{34}$$

$$I(M_n;Z^n)\le\sum_{i=1}^n I(U_i;Z_i|S_i)\,,\tag{35}$$

$$I(K_nM_n;Y^n)\le\sum_{i=1}^n I(X_iU_iS_i;Y_i)\,,\tag{36}$$

$$I(K_nM_n;Z^n)\le\sum_{i=1}^n I(X_iU_i;Z_i|S_i)\,.\tag{37}$$

The bounds (34)-(37) also hold for any stochastic relay encoder. If f_n is a deterministic encoder, we have

$$\begin{aligned}&I(K_n;Z^n|M_n)\\ &\ge\sum_{i=1}^n\left\{I(X_i;Z_i|U_iS_i)-I(U_i;Z_i|X_iS_i)\right\}\,,\end{aligned}\tag{38}$$

$$\begin{aligned}&I(K_n;Y^n|M_n)-I(K_n;Z^n|M_n)\\ &\le\sum_{i=1}^n\left\{I(X_i;Y_i|U_iS_i)-I(X_i;Z_i|U_iS_i)\right\}\,,\end{aligned}\tag{39}$$

in addition to (34)-(37). If Γ belongs to the class NL, the bounds (38) and (39) also hold for any stochastic relay encoder.

Proof of Lemma 8 is in Appendix E.

Proof of $\mathcal{R}_{\rm d}(\Gamma)\subseteq\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$*:* We assume that $(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(\Gamma)$. Let Q, X, Y, Z, S be the same random variables as those in the proof of $\mathcal{R}_{\rm s}(\Gamma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma)$. Set

$$U\stackrel{\triangle}{=}U_QQ=Y_{Q+1}^nZ^{Q-1}M_nQ\,.$$

Note that $UXSYZ$ satisfies a Markov chain $U\to XSZ\to Y$. By Lemmas 7 and 8, we have

$$\left.\begin{aligned}R_0&\le\min\{I(US;Y),I(U;Z|S)\}+\delta_{1,n}\\ R_0+R_1&\le I(X;Y|US)\\ &\quad+\min\{I(US;Y),I(U;Z|S)\}+\tilde{\delta}_{3,n}\\ R_{\rm e}&\le[R_1-I(X;Z|US)\\ &\quad+I(U;Z|XS)]^+\delta_{3,n}\\ R_{\rm e}&\le[I(X;Y|US)-I(X;Z|US)]^++\delta_{4,n}\,.\end{aligned}\right\}\tag{40}$$

By letting $n\to\infty$ in (40), we conclude that $(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$. ■

The following is a key lemma to prove $\mathcal{R}_{\rm d}(\Gamma)\subseteq\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$.

Lemma 9: Set

$$U_i\stackrel{\triangle}{=}Y^{i-1}Z_{i+1}^nM_n\,,\quad i=1,2,\cdots,n\,.$$

For $i=1,2,\cdots,n$, U_i, $X_iS_iZ_i$, and Y_i form a Markov chain $U_i\to X_iZ_iS_i\to Y_i$ in this order. Furthermore, we have

$$I(M_n;Y^n)\le\sum_{i=1}^n I(U_i;Y_i)\,,\tag{41}$$

$$I(M_n;Z^n)\le\sum_{i=1}^n I(U_i;Z_i|S_i)\,,\tag{42}$$

$$I(K_nM_n;Y^n)\le\sum_{i=1}^n I(X_iS_i;Y_i)\,,\tag{43}$$

$$I(K_nM_n;Z^n)\le\sum_{i=1}^n I(X_i;Z_i|S_i)\,.\tag{44}$$

If f_n is a deterministic encoder, we have

$$\begin{aligned}&I(K_n;Z^n|M_n)\\ &\ge\sum_{i=1}^n\left\{I(X_i;Z_i|U_iS_i)-I(U_i;Z_i|X_iS_i)\right\}\,,\end{aligned}\tag{45}$$

$$\begin{aligned}&I(K_n;Y^n|M_n)-I(K_n;Z^n|M_n)\\ &\le\sum_{i=1}^n\{I(X_iS_i;Y_i|U_i)-I(X_iS_i;Z_i|U_i)\\ &\qquad+I(U_i;Z_i|X_iS_i)\}\\ &=\sum_{i=1}^n\{I(X_i;Y_i|U_iS_i)-I(X_i;Z_i|U_iS_i)\\ &\qquad+\zeta(S_i;Y_i,Z_i|U_i)+I(U_i;Z_i|X_iS_i)\}\,,\end{aligned}\tag{46}$$

in addition to (41)-(44). The bounds (41),(43), and (44) also hold for any stochastic relay encoder. If Γ belongs to the class NL, the bound (42) also holds for any stochastic relay encoder. If f_n is deterministic and Γ belongs to the class NL, the bounds (41)-(46) hold for any stochastic relay encoder.

Proof of Lemma 9 is in Appendix F.

Proof of $\mathcal{R}_{\rm d}(\Gamma)\subseteq\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$*:* We assume that $(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(\Gamma)$. Let Q, X, Y, Z, S be the same random variables as those in the proof $\mathcal{R}_{\rm s}(\Gamma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma)$. We set

$$U\stackrel{\triangle}{=}U_QQ=Y^{Q-1}Z_{Q+1}^nM_nQ\,.$$

Note that $UXSYZ$ satisfies a Markov chain $U\to XSZ\to Y$. Furthermore, if Γ belongs to the class NL, we have

$$U\to XS\to Z,\tag{47}$$

which together with $U\to XSZ\to Y$ yields

$$U\to XS\to YZ\,.$$

By Lemmas 7 and 9, we have

$$\left.\begin{aligned}R_0&\le\min\{I(U;Y),I(U;Z|S)\}+\delta_{1,n}\\ R_0+R_1&\le I(X;Y|US)+\min\{I(US;Y),\\ &\quad I(U;Z|S)+\zeta(S;Y,Z|U)\}+\tilde{\delta}_{3,n}\\ R_{\rm e}&\le[R_1-I(X;Z|US)\\ &\quad+I(U;Z|XSQ)]^++\delta_{3,n}\\ &=[R_1-I(X;Z|US)]^++\delta_{3,n}\\ R_{\rm e}&\le[I(XS;Y|U)-I(XS;Z|U)\\ &\quad+I(U;Z|XSQ)]^++\delta_{4,n}\\ &=[I(XS;Y|U)-I(XS;Z|U)]^++\delta_{4,n}\,.\end{aligned}\right\}\tag{48}$$

Note here that since $I(U;Z|XSQ) \le I(U;Z|XS)$ and the Markov chain of (47), the quantity $I(U;Z|XSQ)$ vanishes. By letting $n \to \infty$ in (48), we conclude that $(R_0, R_1,\ R_{\rm e}) \in \hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$. ■

The following is a key result to prove $\mathcal{R}_{\rm s}(\Gamma) \subseteq \mathcal{R}_{\rm s}^{(\rm out)}(\Gamma)$.

Lemma 10: Let U_i, $i = 1, 2, \cdots, n$ be the same random variables as those defined in Lemma 8. We further set $V_i \stackrel{\triangle}{=} U_i S_i K_n$. For $i = 1, 2, \cdots, n$, $U_i V_i X_i S_i Z_i$ satisfies the following Markov chains

$$U_i \to V_i \to X_i S_i Z_i \to Y_i\,, U_i S_i \to V_i X_i \to Z_i\,,$$
$$U_i S_i \to V_i \to X_i\,.$$

Furthermore, we have

$$I(M_n; Y^n) \le \sum_{i=1}^n I(U_i S_i; Y_i)\,, \tag{49}$$

$$I(M_n; Z^n) \le \sum_{i=1}^n I(U_i; Z_i|S_i)\,, \tag{50}$$

$$I(K_n M_n; Y^n) \le \sum_{i=1}^n I(V_i U_i S_i; Y_i)\,, \tag{51}$$

$$I(K_n M_n; Z^n) \le \sum_{i=1}^n I(V_i U_i; Z_i|S_i)\,, \tag{52}$$

$$\begin{aligned} &I(K_n; Y^n|M_n) - I(K_n; Z^n|M_n) \\ &= \sum_{i=1}^n \{I(V_i; Y_i|U_i S_i) - I(V_i; Z_i|U_i S_i)\}\,. \end{aligned} \tag{53}$$

The bounds (49)-(52) also hold for any stochastic relay encoder. If Γ belongs to the class NL, the bound (53) also holds for any stochastic relay encoder.

Proof of Lemma 10 is given in Appendix E.

Proof of $\mathcal{R}_{\rm s}(\Gamma) \subseteq \mathcal{R}_{\rm s}^{(\rm out)}(\Gamma)$*:* Let Q, X, Y, Z, S, U be the same random variables as those in the proof of $\mathcal{R}_{\rm d}(\Gamma) \subseteq \mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$. We further set $V \stackrel{\triangle}{=} USK_n$. Note that $UVXSZ$ satisfies the following Markov chains

$$U \to V \to XSZ \to Y\,, US \to VX \to Z\,,$$
$$US \to V \to X\,.$$

By Lemmas 7 and 10, we have

$$\left.\begin{aligned} R_0 &\le \min\{I(US;Y), I(U;Z|S)\} + \delta_{1,n} \\ R_0 + R_1 &\le I(V;Y|US) \\ &\quad + \min\{I(US;Y), I(U;Z|S)\} + \tilde{\delta}_{3,n} \\ R_{\rm e} &\le R_1 + \delta_{3,n} \\ R_{\rm e} &\le I(V;Y|US) - I(V;Z|US) + \delta_{4,n}\,. \end{aligned}\right\} \tag{54}$$

By letting $n \to \infty$ in (54), we conclude that $(R_0, R_1, R_{\rm e}) \in \mathcal{R}_{\rm s}^{(\rm out)}(\Gamma)$. ■

Proof of Theorem 6: We assume that Γ belongs to the class NL. By Lemmas 5-10 and arguments quite parallel with the previous arguments of the derivations of outer bounds we can prove that $\mathcal{R}_{\rm d}^{(\rm out)}(\Gamma)$, $\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$, and $\hat{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$ serve as outer bounds of $\mathcal{R}_{\rm d}^{*}(\Gamma)$ and that $\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma)$ and $\mathcal{R}_{\rm s}^{(\rm out)}(\Gamma)$ serve as outer bounds of $\mathcal{R}_{\rm s}^{*}(\Gamma)$. ■

VIII. Derivations of the Inner and Outer Bounds for the Gaussian Relay Channel

In this section we prove Theorem 7. Let (ξ_1, ξ_2) be a zero mean Gaussian random vector with covariance Σ defined in Section V. By definition, we have

$$\xi_2 = \rho\sqrt{\frac{N_2}{N_1}}\xi_1 + \xi_{2|1}\,,$$

where $\xi_{2|1}$ is a zero mean Gaussian random variable with variance $(1-\rho^2)N_2$ and independent of ξ_1. We consider the Gaussian relay channel specified by Σ. For two input random variables X and S of this Gaussian relay channel, output random variables Y and Z are given by

$$\begin{aligned} Y &= X + S + \xi_1\,, \\ Z &= X + \xi_2 = X + \rho\sqrt{\frac{N_2}{N_1}}\xi_1 + \xi_{2|1}\,. \end{aligned}$$

Define two sets of random variables by

$$\begin{aligned} \mathcal{P}(P_1, P_2) \stackrel{\triangle}{=} \{(U,X,S):\ &\mathbf{E}[X^2] \le P_1, \mathbf{E}[S^2] \le P_2\,, \\ &U \to XS \to YZ\,\}\,, \end{aligned}$$

$$\begin{aligned} \mathcal{P}_G(P_1, P_2) \stackrel{\triangle}{=} \{(U,X,S):\ &U, X, S \text{ are zero mean} \\ &\text{Gaussian random variables.} \\ &\mathbf{E}[X^2] \le P_1\,, \mathbf{E}[S^2] \le P_2\,, \\ &U \to XS \to YZ\,\}\,. \end{aligned}$$

Set

$$\begin{aligned} \tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(P_1, P_2|\Sigma) \stackrel{\triangle}{=} \{&(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\ &R_1 \le I(X;Y|US)\,, \\ &R_{\rm e} \le [R_1 - I(X;Z|US)]^+\,, \\ &\text{for some } (U,X,S) \in \mathcal{P}_G(P_1,P_2)\,.\}\,, \end{aligned}$$

$$\begin{aligned} \tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(P_1, P_2|\Sigma) \stackrel{\triangle}{=} \{&(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0\,, \\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\ &R_1 \le I(X;YZ|US)\,, \\ &R_0 + R_1 \le I(XS;Y)\,, \\ &R_{\rm e} \le [R_1 - I(X;Z|US)]^+\,, \\ &R_{\rm e} \le I(X;Y|ZUS)\,, \\ &\text{for some } (U,X,S) \in \mathcal{P}(P_1,P_2)\,.\}, \end{aligned}$$

$$\begin{aligned} \tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(P_1, P_2|\Sigma) \stackrel{\triangle}{=} \{&(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0, \\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\ &R_{\rm e} \le R_1 \le I(X;Y|US)\,, \\ &R_{\rm e} \le I(X;Y|US) - I(X;Z|US)\,, \\ &\text{for some } (U,X,S) \in \mathcal{P}_G(P_1,P_2)\,.\}\,, \end{aligned}$$

$$\begin{aligned} \tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(P_1, P_2|\Sigma) \stackrel{\triangle}{=} \{&(R_0, R_1, R_{\rm e}) : R_0, R_1, R_{\rm e} \ge 0, \\ &R_0 \le \min\{I(US;Y), I(U;Z|S)\}\,, \\ &R_0 + R_1 \le I(XS;Y)\,, \\ &R_{\rm e} \le R_1 \le I(X;YZ|US)\,, \\ &R_{\rm e} \le I(X;Y|ZUS)\,, \\ &\text{for some } (U,X,S) \in \mathcal{P}(P_1,P_2)\,.\}. \end{aligned}$$

Then we have the following.

Proposition 1: For any Gaussian relay channel we have

$$\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)\subseteq\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(P_1,P_2|\Sigma),$$
$$\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(P_1,P_2|\Sigma).$$

Proof: The first and third inclusions in the above proposition can be proved by a method quite similar to that in the case of discrete memoryless channels. In the Gaussian case we replace the entropy $H(Z|XS)$ appearing in the definition of $B_{Z|XS,\epsilon}$ by the differential entropy $h(Z|XS)$. Similarly, we replace the entropy $H(Z|US)$ appearing in the definition of $B_{Z|US,\epsilon}$ by the differential entropy $h(Z|US)$. On the other hand, Lemma 3 should be replaced by the following lemma.

Lemma 11: For any Gaussian relay channels and for $i=1,2,\cdots,B-1$, we have

$$\begin{aligned}&\frac{1}{n}H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\ &\geq r_1-I(X;Z|US)-2\epsilon-\frac{3+\log\mathrm{e}}{n}\\ &\quad-\left[e_{Z|US,i}^{(n)}+\sqrt{(P_1+N_2)e_{Z|US,i}^{(n)}}\right]\\ &\quad-\left\{\tfrac{1}{2}\log(2\pi\mathrm{e}N_2)\right\}e_{Z|XS,i}^{(n)}.\end{aligned}$$

Proof of this lemma is in Appendix B. Using Lemma 11, we can prove that Lemma 2 still holds in the case of Gaussian relay channels. Using this lemma, we can prove the first and third inclusions in Proposition 1. We omit the detail of the proof.

We next prove the second and fourth inclusions in Proposition 1. Let Q, X, Y, Z, S, U be the same random variables as those in the proofs of $\mathcal{R}_{\rm d}(\Gamma)\subseteq\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(\Gamma)$ in Theorem 1 and $\mathcal{R}_{\rm s}(\Gamma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(\Gamma)$ in Theorem 4. Note that $UXSYZ$ satisfies a Markov chain $U\to XS\to YZ$. We assume that $(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm s}(P_1,P_2|\Sigma)$. On the power constraint on X, we have

$$\mathbf{E}\left[X^2\right]=\frac{1}{n}\sum_{i=1}^{n}\mathbf{E}\left[X_i^2\right]\leq P_1\,.$$

Similarly, we obtain $\mathbf{E}\left[S^2\right]\leq P_2$. Hence, we have $(U,X,S)\in\mathcal{P}(P_1,P_2)$. By Lemmas 5 and 6, we have (29). Hence, by letting $n\to\infty$, we obtain $(R_0,R_1,R_{\rm e})\in\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(P_1,P_2|\Sigma)$. Next we assume that $(R_0,R_1,R_{\rm e})\in\mathcal{R}_{\rm d}(P_1,P_2|\Sigma)$. We also have $(U,X,S)\in\mathcal{P}(P_1,P_2)$. By Lemmas 5 and 6, we have (29) and (30). Hence, by letting $n\to\infty$, we obtain $(R_0,R_1,R_{\rm e})\in\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(P_1,P_2|\Sigma)$. ∎

It can be seen from Proposition 1 that to prove Theorem 7, it suffices to prove

$$\left.\begin{aligned}&\mathcal{R}_{\rm d}^{(\rm in)}(P_1,P_2|\Sigma)\subseteq\tilde{\mathcal{R}}_{\rm d}^{(\rm in)}(P_1,P_2|\Sigma)\\ &\mathcal{R}_{\rm s}^{(\rm in)}(P_1,P_2|\Sigma)\subseteq\tilde{\mathcal{R}}_{\rm s}^{(\rm in)}(P_1,P_2|\Sigma)\end{aligned}\right\}\tag{55}$$

$$\left.\begin{aligned}&\tilde{\mathcal{R}}_{\rm d}^{(\rm out)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm d}^{(\rm out)}(P_1,P_2|\Sigma)\\ &\tilde{\mathcal{R}}_{\rm s}^{(\rm out)}(P_1,P_2|\Sigma)\subseteq\mathcal{R}_{\rm s}^{(\rm out)}(P_1,P_2|\Sigma).\end{aligned}\right\}\tag{56}$$

Proof of (55) is straightforward. To prove (56), we need some preparations. Set

$$a\stackrel{\triangle}{=}\tfrac{N_2-\rho\sqrt{N_1N_2}}{N_1+N_2-2\rho\sqrt{N_1N_2}}\,.$$

Define random variables $\tilde{Y}$, $\tilde{\xi}_1$, and $\tilde{\xi}_2$ by

$$\begin{aligned}\tilde{Y}&\stackrel{\triangle}{=}aY+\bar{a}Z\,,\\ \tilde{\xi}_1&\stackrel{\triangle}{=}a\xi_1+\bar{a}\xi_2=\tfrac{(1-\rho^2)N_2\xi_1+(N_1-\rho\sqrt{N_1N_2})\xi_{2|1}}{N_1+N_2-2\rho\sqrt{N_1N_2}}\,,\\ \tilde{\xi}_2&\stackrel{\triangle}{=}\xi_1-\xi_2=\left(1-\rho\sqrt{\tfrac{N_2}{N_1}}\right)\xi_1-\xi_{2|1}\,.\end{aligned}$$

Let $\tilde{N}_i=\mathbf{E}[\tilde{\xi}_i^2],i=1,2$. Then, by simple computation we can show that $\tilde{\xi}_1$ and $\tilde{\xi}_2$ are independent Gaussian random variables and

$$\begin{aligned}\tilde{N}_1&=\tfrac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}\,,\\ \tilde{N}_2&=N_1+N_2-2\rho\sqrt{N_1N_2}\,.\end{aligned}$$

We have the following relations between $\tilde{Y}$, Y, and Z:

$$\left.\begin{aligned}\tilde{Y}&=X+aS+\tilde{\xi}_1\\ Y&=\tilde{Y}+\bar{a}(S+\tilde{\xi}_2)\\ Z&=\tilde{Y}-a(S+\tilde{\xi}_2).\end{aligned}\right\}\tag{57}$$

The following is a useful lemma to prove (56).

Lemma 12: Suppose that $(U,X,S)\in\mathcal{P}(P_1,P_2)$. Let $X(s)$ be a random variable with a conditional distribution of X for given $S=s$. $\mathbf{E}_{X(s)}[\cdot]$ stands for the expectation with respect to the (conditional) distribution of $X(s)$. Then, there exists a pair $(\alpha,\beta)\in[0,1]^2$ such that

$$\begin{aligned}\mathbf{E}_S\left(\mathbf{E}_{X(S)}X(S)\right)^2&=\bar{\alpha}P_1\,,\\ h(Y|S)&\leq\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})(\alpha P_1+N_1)\right\}\,,\\ h(Z|S)&\leq\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})(\alpha P_1+N_2)\right\}\,,\\ h(Y)&\leq\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})(P_1+P_2+2\sqrt{\bar{\alpha}P_1P_2}+N_1)\right\}\,,\\ h(\tilde{Y}|US)&=\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})(\beta\alpha P_1+\tilde{N}_1)\right\}\,,\\ h(Y|US)&\geq\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1+N_1\right)\right\}\,,\\ h(Z|US)&\geq\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1+N_2\right)\right\}\,.\end{aligned}$$

Proof of Lemma 12 is given in Appendix G. Using this lemma, we can prove Theorem 7.

Proof of Theorem 7: We first prove (55). Choose $(U,X,S)\in\mathcal{P}_G$ such that

$$\begin{aligned}&\mathbf{E}[X^2]=P_1,\quad\mathbf{E}[S^2]=P_2,\\ &U=\sqrt{\tfrac{\bar{\theta}\bar{\eta}P_1}{P_2}}S+\tilde{U},\quad X=U+\tilde{X},\end{aligned}$$

where $\tilde{U}$ and $\tilde{X}$ are zero mean Gaussian random variables with variance $\bar{\theta}\eta P_1$ and θP_1, respectively. The random variables S, $\tilde{U}$, and $\tilde{X}$ are independent. For the above choice of (U,X,S), we have

$$\begin{aligned}I(US;Y)&=C\left(\tfrac{\bar{\theta}P_1+P_2+2\sqrt{\bar{\theta}\bar{\eta}P_1P_2}}{\theta P_1+N_1}\right)\,,\\ I(U;Z|S)&=C\left(\tfrac{\bar{\theta}\eta P_1}{\theta P_1+N_2}\right)\,,\\ I(X;Y|US)&=C\left(\tfrac{\theta P_1}{N_1}\right)\,,\quad I(X;Z|US)=C\left(\tfrac{\theta P_1}{N_2}\right)\,.\end{aligned}$$

Thus, (55) is proved. Next, we prove (56). By Lemma 12, we

have

$$\begin{aligned} I(US;Y) &= h(Y) - h(Y|US) \\ &\le C\left(\tfrac{(1-\beta\alpha)P_1+P_2+2\sqrt{\bar{\alpha}P_1P_2}}{\beta\alpha P_1+N_1}\right), \quad (58) \\ I(U;Z|S) &= h(Z|S) - h(Z|US) \\ &\le C\left(\tfrac{\bar{\alpha}P_1}{\beta\alpha P_1+N_2}\right), \quad (59) \\ I(XS;Y) &= h(Y) - h(Y|XS) \\ &\le C\left(\tfrac{(1-\beta\alpha)P_1+P_2+2\sqrt{\bar{\alpha}P_1P_2}}{N_1}\right), \quad (60) \\ I(X;Z|US) &= h(Z|US) - h(Z|XS) \\ &\ge C\left(\tfrac{\beta\alpha P_1}{N_2}\right), \quad (61) \\ I(X;YZ|US) &= h(YZ|US) - h(YZ|XS) \\ &= h(\tilde{Y}Z|US) - h(\tilde{Y}Z|XS) \\ &= h(\tilde{Y}|US) + h(Z|\tilde{Y}US) \\ &\quad -h(\tilde{Y}|XS) - h(Z|\tilde{Y}XS) \\ &\overset{(a)}{=} h(\tilde{Y}|US) - h(\tilde{Y}|XS) \\ &= C\left(\frac{\beta\alpha P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right), \quad (62) \end{aligned}$$

where (a) follows from

$$\begin{aligned} &h(Z|\tilde{Y}US) = h(Z|\tilde{Y}XS) = h(Z|\tilde{Y}S) \\ &= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})a^2\tilde{N}_2\right\}. \end{aligned}$$

From (61) and (62), we have

$$I(X;Y|ZUS) \le C\left(\frac{\beta\alpha P_1}{\frac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}}\right) - C\left(\tfrac{\beta\alpha P_1}{N_2}\right). \quad (63)$$

Here we transform the variable pair $(\alpha,\beta) \in [0,1]^2$ into $(\eta,\theta) \in [0,1]^2$ in the following manner:

$$\theta = \beta\alpha, \quad \eta = 1 - \frac{\bar{\alpha}}{\bar{\theta}} = \frac{\alpha-\theta}{1-\theta}. \quad (64)$$

This map is a bijection because from (64), we have

$$\alpha = 1 - \bar{\theta}\bar{\eta} \ge \theta, \quad \beta = \frac{\theta}{\alpha}. \quad (65)$$

Combining (58)-(60), (62), (63), and (65), we have (56). ■

IX. Conclusion

We have considered the coding problem of the RCC, where the relay acts as both a helper and a wire-tapper. We have derived the inner and outer bounds of the deterministic and stochastic rate-equivocation regions of the RCC and have established the deterministic rate region in the case where the relay channel is reversely degraded. Furthermore, we have computed the inner and outer bounds of the deterministic and stochastic secrecy capacities and have determined the deterministic secrecy capacity for the class of reversely degraded relay channels. We have also evaluated the rate-equivocation region and secrecy capacity in the case of Gaussian relay channels.

In this paper, we have focused purely on the derivation of information-theoretic bounds on the RCC. Problem of practical constructions of codes achieving the derived inner bounds of the RCC is left to us as a further study. Applications of LDPC codes to the wire-tap channel were studied in [31]. This work may provide some key ideas to investigate the code design problem for the RCC.

Appendix

In the following arguments, $X_{[i]}$ stands for $(X^{i-1},\, X_{i+1}^n)$. Similar notations are used for other random variables.

A. Proof of Lemma 2

In this appendix we prove Lemma 2.

Proof of Lemma 2: We first derive the upper bound of $\mathsf{E}\left[\hat{e}_{2,i}^{(n)}(1|w_i)\right]$ in Lemma 2. Set

$$\begin{aligned} &\tilde{e}_{2,i}^{(n)} \triangleq \Pr\{\tilde{\mathcal{E}}_{2,i}|\mathcal{F}_{i-1}^c\}, \hat{e}_{2,i}^{(n)} \triangleq \Pr\{\hat{\mathcal{E}}_{2,i}|\mathcal{F}_{i-1}^c\}, \\ &\tilde{e}_{2,i}^{(n)}(t_i|\phi_n(t_{i-1}), l_i) \\ &\triangleq \Pr\{\tilde{\mathcal{E}}_{2,i}|\mathcal{F}_{i-1}^c,\, T_{n,i}=t_i, T_{n,i-1}=t_{i-1}, \\ &\qquad J_{n,i}=j_i, L_{n,i}=l_i\}, \\ &\hat{e}_{2,i}^{(n)}(t_i|\phi_n(t_{i-1})) \\ &\triangleq \Pr\{\hat{\mathcal{E}}_{2,i}|\mathcal{F}_{i-1}^c, T_{n,i}=t_i, T_{n,i-1}=t_{i-1}\}. \end{aligned}$$

Similar notations are used for other error probabilities. By definition of $\tilde{e}_{2,i}^{(n)}$ and $\hat{e}_{2,i}^{(n)}$, we have

$$\left.\begin{aligned} &\mathsf{E}\left[e_{2,i}^{(n)}\right] \le \mathsf{E}\left[\hat{e}_{2,i}^{(n)}\right] + \mathsf{E}\left[\tilde{e}_{2,i}^{(n)}\right] \\ &\mathsf{E}\left[\tilde{e}_{2,i}^{(n)}\right] = \frac{1}{|\mathcal{T}_n|^2|\mathcal{J}_n||\mathcal{L}_n|} \\ &\qquad \times \sum_{\substack{(t_i,t_{i-1},j_i,l_i) \\ \in\mathcal{T}_n^2\times\mathcal{J}_n\times\mathcal{L}_n}} \mathsf{E}\left[\tilde{e}_{2,i}^{(n)}(t_i|\phi_n(t_{i-1}),j_i,l_i)\right] \\ &\mathsf{E}\left[\hat{e}_{2,i}^{(n)}\right] = \frac{1}{|\mathcal{T}_n|^2} \sum_{(t_i,t_{i-1})\in\mathcal{T}_n^2} \mathsf{E}\left[\hat{e}_{2,i}^{(n)}(t_i|\phi_n(t_{i-1}))\right]. \end{aligned}\right\} \quad (66)$$

By the symmetrical property of random coding, it suffices to evaluate $\mathsf{E}[\tilde{e}_{2,i}^{(n)}\ (1|\phi_n(t_{i-1}),1,1)]$ and $\mathsf{E}[\hat{e}_{2,i}^{(n)}\ (1|\phi_n(t_{i-1}))]$. Note that

$$\begin{aligned} &\mathsf{E}\left[\tilde{e}_{2,i}^{(n)}(1|\phi_n(t_{i-1}),1,1)\right] \\ &= \sum_{w_i\in\mathcal{W}_n} \mathsf{E}\left[\tilde{e}_{2,i}^{(n)}(1|w_i,1,1)\middle|\,\phi_n(t_{i-1})=w_i\right]\frac{1}{|\mathcal{W}_n|}, \quad (67) \\ &\mathsf{E}\left[\hat{e}_{2,i}^{(n)}(1|\phi_n(t_{i-1}))\right] \\ &= \sum_{w_i\in\mathcal{W}_n} \mathsf{E}\left[\hat{e}_{2,i}^{(n)}(1|w_i)\middle|\,\phi_n(t_{i-1})=w_i\right]\frac{1}{|\mathcal{W}_n|}. \quad (68) \end{aligned}$$

On $\mathsf{E}[\tilde{e}_{2,i}^{(n)}\ (1|w_i,1,1)\ |\phi_n(t_{i-1})=w_i]$, we have the following.

$$\begin{aligned} &\mathsf{E}\left[\tilde{e}_{2,i}^{(n)}(1|w_i,1,1)\middle|\,\phi_n(t_{i-1})=w_i\right] \\ &= \sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,1),\\ \boldsymbol{z}_i)\notin\mathcal{A}_{UZ|S,\epsilon}}} \sum_{\boldsymbol{x}(w_i,1,1,1)\in\mathcal{X}^n} p_S(\boldsymbol{s}(w_i))p_{U|S}(\boldsymbol{u}(w_i,1)|\boldsymbol{s}(w_i)) \\ &\qquad \times p_{X|US}(\boldsymbol{x}(w_i,1,1,1)|\boldsymbol{u}(w_i,1),\boldsymbol{s}(w_i)) \\ &\qquad \times p_{Z|XS}(\boldsymbol{z}_i|\boldsymbol{x}(w_i,1,1,1),\boldsymbol{s}(w_i)) \end{aligned}$$

$$= \sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,1),\\ \boldsymbol{z}_i)\notin\mathcal{A}_{UZ|S,\epsilon}}} p_S(\boldsymbol{s}(w_i))p_{UZ|S}(\boldsymbol{u}(w_i,1),\boldsymbol{z}_i|\boldsymbol{s}(w_i))$$
$$= \Pr\left\{(S^n,U^n,Z^n)\notin\mathcal{A}_{UZ|S,\epsilon}\right\}. \tag{69}$$

From (67) and (69), we have

$$\mathsf{E}\left[\tilde{e}^{(n)}_{2,i}(1|\phi_n(t_{i-1}),1)\right] = \Pr\left\{(S^n,U^n,Z^n)\notin\mathcal{A}_{UZ|S,\epsilon}\right\}. \tag{70}$$

On $\mathsf{E}[\hat{e}^{(n)}_{2,i}\ (1|w_i)\ |\phi_n(t_{i-1})=w_i]$, we have the following.

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}^{(n)}_{2,i}(1|w_i)\middle|\phi_n(t_{i-1})=w_i\right]\\
&\le \sum_{\hat{t}_i\neq 1}\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{t}_i),\\ \boldsymbol{z}_i)\in\mathcal{A}_{UZ|S,\epsilon}}} p_S(\boldsymbol{s}(w_i))p_{U|S}(\boldsymbol{u}(w_i,\hat{t}_i)|\boldsymbol{s}(w_i))\\
&\qquad\times p_{Z|S}(\boldsymbol{z}_i|\boldsymbol{s}(w_i))\\
&\overset{(a)}{\le} \sum_{\hat{t}_i\neq 1}\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{t}_i),\\ \boldsymbol{z}_i)\in\mathcal{A}_{UZ|S,\epsilon}}} p_S(\boldsymbol{s}(w_i))p_{UZ|S}(\boldsymbol{u}(w_i,t_i),\boldsymbol{z}_i|\boldsymbol{s}(w_i))\\
&\qquad\times 2^{-n[R_0+\epsilon]}\\
&= \sum_{\hat{t}_i\neq 1} 2^{-n[R_0+\epsilon]}\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{t}_i),\\ \boldsymbol{z}_i)\in\mathcal{A}_{UZ|S,\epsilon}}} p_{SUZ}(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{t}_i),\boldsymbol{z}_i)\\
&\le 2^{-n[R_0+\epsilon]}(2^{nR_0}-1)\le 2^{-n\epsilon}.
\end{aligned} \tag{71}$$

Step (a) follows from the definition of $\mathcal{A}_{UZ|S,\epsilon}$. From (68) and (71), we have

$$\mathsf{E}\left[\hat{e}^{(n)}_{2,i}(1|\phi_n(t_{i-1}))\right]\le 2^{-n\epsilon}. \tag{72}$$

Hence, form (66), (70), and (72) we have

$$\mathsf{E}\left[\hat{e}^{(n)}_{2,i}\right]\le \Pr\left\{(S^n,U^n,Z^n)\notin\mathcal{A}_{UZ|S,\epsilon}\right\}+2^{-n\epsilon}.$$

In a manner quite similar to the above argument, we can derive the upper bounds of $\mathsf{E}\left[e^{(n)}_{1\mathrm{a},i}\right]$ and $\mathsf{E}\left[e^{(n)}_{1\mathrm{c},i}\right]$ stated in Lemma 2.

Next, we derive the upper bound of $\mathsf{E}\left[e^{(n)}_{1\mathrm{b},i}\right]$. By definition of $\tilde{e}^{(n)}_{1\mathrm{b},i}$ and $\hat{e}^{(n)}_{1\mathrm{b},i}$, we have

$$\left.\begin{aligned}
&\mathsf{E}\left[e^{(n)}_{1\mathrm{b},i}\right]\le \mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}\right]+\mathsf{E}\left[\tilde{e}^{(n)}_{1\mathrm{b},i}\right]\\
&\mathsf{E}\left[\tilde{e}^{(n)}_{1\mathrm{b},i}\right] = \frac{1}{|\mathcal{T}_n|^2|\mathcal{L}_n|}\\
&\qquad\times\sum_{\substack{(t_{i-1},t_{i-2},\\ l_{i-1})\in\mathcal{T}_n^2\times\mathcal{L}_n}}\mathsf{E}\left[\tilde{e}^{(n)}_{1\mathrm{b},i}(t_{i-1}|\phi_n(t_{i-2}),l_{i-1})\right]\\
&\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}\right] = \frac{1}{|\mathcal{T}_n|^2}\sum_{(t_{i-1},t_{i-2})\in\mathcal{T}_n^2}\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(t_{i-1}|\phi_n(t_{i-2}))\right].
\end{aligned}\right\} \tag{73}$$

By the same argument as that of the derivation of (70), we have

$$\begin{aligned}
&\mathsf{E}\left[\tilde{e}^{(n)}_{1\mathrm{b},i}(t_{i-1}|\phi_n(t_{i-2}),l_{i-1})\right]\\
&\quad=\Pr\left\{(S^n,U^n,Y^n)\notin\mathcal{A}_{UY|S,\epsilon}\right\}
\end{aligned} \tag{74}$$

for any $(t_{i-1},t_{i-2},l_{i-1})\in\mathcal{T}_n^2\times\mathcal{L}_n$. Then, from (73) and (74), we have

$$\mathsf{E}\left[\tilde{e}^{(n)}_{1\mathrm{b},i}\right]=\Pr\left\{(S^n,U^n,Y^n)\notin\mathcal{A}_{UY|S,\epsilon}\right\}. \tag{75}$$

Next, we evaluate $\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(t_{i-1}|\phi_n(t_{i-2}))\right]$. By the symmetrical property of random coding, it suffices to evaluate the above quantity for $(t_{i-1},t_{i-2})=(1,1)$ or $(1,2)$. When $(t_{i-1},t_{i-2})=(1,1)$, set $\phi_n(1)=w_i$. Then, we have

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|\phi_n(1))\right]=\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_i)\right]\\
&\le\sum_{\hat{\hat{t}}_{i-1}\neq 1}\sum_{w_i\in\mathcal{W}_n}\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_i)\middle|\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i\right]\\
&\qquad\times\Pr\left\{\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i\right\}\\
&=\sum_{\hat{\hat{t}}_{i-1}\neq 1}\sum_{w_i\in\mathcal{W}_n}\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_i)\middle|\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i\right]\\
&\qquad\times\frac{1}{|\mathcal{W}_n|^2}.
\end{aligned} \tag{76}$$

On upper bound of

$$\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_i)\middle|\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i\right],$$

we have the following chain of inequalities:

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_i)\middle|\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i\right]\\
&\le\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_i))\\
&\qquad\times p_{U|S}(\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1})|\boldsymbol{s}(w_i))p_{Y|S}(\boldsymbol{y}_i|\boldsymbol{s}(w_i))\\
&\overset{(a)}{\le}\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_i))\\
&\qquad\times p_{UY|S}(\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\boldsymbol{y}_{i-1}|\boldsymbol{s}(w_i))2^{-n[R_0-r+\epsilon]}\\
&=2^{-n[R_0-r+\epsilon]}\\
&\qquad\times\sum_{\substack{(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_{SUY}(\boldsymbol{s}(w_i),\boldsymbol{u}(w_i,\hat{\hat{t}}_{i-1}),\boldsymbol{y}_{i-1})\\
&\le 2^{-n[R_0-r+\epsilon]}.
\end{aligned} \tag{77}$$

Step (a) follows from the definition of $\mathcal{A}_{UY|S,\epsilon}$. It follows from (76) and (77) that when $(t_{i-1},t_{i-2})=(1,1)$, we have

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|\phi_n(1))\right]\le\sum_{\hat{\hat{t}}_{i-1}\neq 1}\sum_{w_i\in\mathcal{W}_n}\frac{2^{-n[R_0-r+\epsilon]}}{|\mathcal{W}_n|^2}\\
&\le(2^{nR_0}-1)\frac{2^{-n[R_0-r+\epsilon]}}{|\mathcal{W}_n|}\le 2\cdot 2^{-n\epsilon}.
\end{aligned} \tag{78}$$

When $(t_{i-1},t_{i-2})=(1,2)$, set $\phi_n(1)=w_i$ and $\phi_n(2)=w_{i-1}$. Then, we have

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|\phi_n(2))\right]=\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_{i-1})\right]\\
&\le\sum_{\hat{\hat{t}}_{i-1}\neq 1}\sum_{(w_i,w_{i-1})\in\mathcal{W}_n^2}\mathsf{E}\left[\hat{e}^{(n)}_{1\mathrm{b},i}(1|w_{i-1})\middle|\begin{aligned}&\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})\\ &\quad=w_i,\\ &\phi_n(2)=w_{i-1}\end{aligned}\right]\\
&\qquad\times\Pr\left\{\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i,\phi_n(2)=w_{i-1}\right\}
\end{aligned}$$

$$= \sum_{\hat{\hat{t}}_{i-1}\neq 1,2} \sum_{(w_i,w_{i-1})\in\mathcal{W}_n^2} \mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\begin{array}{l}\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})\\ =w_i,\\ \phi_n(2)=w_{i-1}\end{array}\right] \times\frac{1}{|\mathcal{W}_n|^3}$$
$$+ \sum_{w_i=w_{i-1}\in\mathcal{W}_n} \mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\begin{array}{l}\phi_n(1)=\phi_n(2)=w_i,\\ \phi_n(2)=w_{i-1}\end{array}\right] \times\frac{1}{|\mathcal{W}_n|^2}. \quad (79)$$

On upper bound of

$$\mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\,\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i,\phi_n(2)=w_{i-1}\right],$$

we have the following chain of inequalities:

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\,\phi_n(1)=\phi_n(\hat{\hat{t}}_{i-1})=w_i,\phi_n(2)=w_{i-1}\right]\\
&\le \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_{i-1}))\\
&\quad\times p_{U|S}(\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1})|\boldsymbol{s}(w_{i-1}))p_{Y|S}(\boldsymbol{y}_i|\boldsymbol{s}(w_{i-1}))\\
&\overset{(a)}{\le} \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_{i-1}))\\
&\quad\times p_{UY|S}(\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}),\boldsymbol{y}_{i-1}|\boldsymbol{s}(w_{i-1}))2^{-n[R_0-r+\epsilon]}\\
&= 2^{-n[R_0-r+\epsilon]}\\
&\quad\times \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_{SUY}(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},\hat{\hat{t}}_{i-1}),\boldsymbol{y}_{i-1})\\
&\le 2^{-n[R_0-r+\epsilon]}. \quad (80)
\end{aligned}$$

Step (a) follows from the definition of $\mathcal{A}_{UY|S,\epsilon}$. On upper bound of

$$\mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\,\phi_n(1)=\phi_n(2)=w_i,\phi_n(2)=w_{i-1}\right],$$

we have the following chain of inequalities:

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|w_{i-1})\middle|\,\phi_n(1)=\phi_n(2)=w_i,\phi_n(2)=w_{i-1}\right]\\
&= \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},2),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_{i-1}))\\
&\quad\times p_{U|S}(\boldsymbol{u}(w_{i-1},2)|\boldsymbol{s}(w_{i-1}))p_{Y|S}(\boldsymbol{y}_i|\boldsymbol{s}(w_{i-1}))\\
&\overset{(a)}{\le} \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},2),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_S(\boldsymbol{s}(w_{i-1}))\\
&\quad\times p_{UY|S}(\boldsymbol{u}(w_{i-1},2),\boldsymbol{y}_{i-1}|\boldsymbol{s}(w_{i-1}))2^{-n[R_0-r+\epsilon]}\\
&= 2^{-n[R_0-r+\epsilon]}\\
&\quad\times \sum_{\substack{(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},2),\\ \boldsymbol{y}_{i-1})\in\mathcal{A}_{UY|S,\epsilon}}} p_{SUY}(\boldsymbol{s}(w_{i-1}),\boldsymbol{u}(w_{i-1},2),\boldsymbol{y}_{i-1})\\
&\le 2^{-n[R_0-r+\epsilon]}. \quad (81)
\end{aligned}$$

Step (a) follows from the definition of $\mathcal{A}_{UY|S,\epsilon}$. It follows from (79)-(81) that when $(t_{i-1},t_{i-2})=(1,2)$, we have

$$\begin{aligned}
&\mathsf{E}\left[\hat{e}_{1\mathrm{b},i}^{(n)}(1|\phi_n(2))\right] \le \sum_{\hat{\hat{t}}_{i-1}\neq 1,2}\sum_{(w_i,w_{i-1})\in\mathcal{W}_n^2}\frac{2^{-n[R_0-r+\epsilon]}}{|\mathcal{W}_n|^3}\\
&+\sum_{w_i=w_{i-1}\in\mathcal{W}_n}\frac{2^{-n[R_0-r+\epsilon]}}{|\mathcal{W}_n|^2}\\
&=(2^{nR_0}-1)\frac{2^{-n[R_0-r+\epsilon]}}{|\mathcal{W}_n|}\le 2\cdot 2^{-n\epsilon}. \quad (82)
\end{aligned}$$

From (73), (75), (78), and (82), we have

$$\mathsf{E}\left[e_{1\mathrm{b},i}^{(n)}\right]\le \Pr\left\{(S^n,U^n,Y^n)\notin\mathcal{A}_{UY|S,\epsilon}\right\}+2\cdot 2^{-n\epsilon}.$$

To derive the upper bound of $\mathsf{E}\left[e_i^{(n)}\right]$ in Lemma 2, set

$$\begin{aligned}
&\tilde{e}_i^{(n)}\triangleq\Pr\{\tilde{\mathcal{E}}_i\},\hat{e}_i^{(n)}\triangleq\Pr\{\hat{\mathcal{E}}_i\},\\
&\tilde{e}_i^{(n)}(j_i|\phi_n(t_{i-1}),t_i,l_i)\\
&\triangleq\Pr\{\tilde{\mathcal{E}}_i|\,T_{n,i}=t_i,T_{n,i-1}=t_{i-1},J_{n,i}=j_i,L_{n,i}=l_i\},\\
&\hat{e}_i^{(n)}(j_i|\phi_n(t_{i-1}),t_i,l_i)\\
&\triangleq\Pr\{\hat{\mathcal{E}}_i|\,T_{n,i}=t_i,T_{n,i-1}=t_{i-1},J_{n,i}=j_i,L_{n,i}=l_i\}.
\end{aligned}$$

By definition of $\tilde{e}_i^{(n)}$ and $\hat{e}_i^{(n)}$, we have

$$\left.\begin{aligned}
&\mathsf{E}\left[e_i^{(n)}\right]\le\mathsf{E}\left[\hat{e}_i^{(n)}\right]+\mathsf{E}\left[\tilde{e}_i^{(n)}\right]\\
&\mathsf{E}\left[\tilde{e}_i^{(n)}\right]=\frac{1}{|\mathcal{T}_n|^2|\mathcal{J}_n||\mathcal{L}_n|}\\
&\qquad\times\sum_{\substack{(t_i,t_{i-1},j_i,l_i)\\ \in\mathcal{T}_n^2\times\mathcal{J}_n\times\mathcal{L}_n}}\mathsf{E}\left[\tilde{e}_i^{(n)}(j_i|\phi_n(t_{i-1}),t_i,l_i)\right]\\
&\mathsf{E}\left[\hat{e}_i^{(n)}\right]=\frac{1}{|\mathcal{T}_n|^2|\mathcal{J}_n||\mathcal{L}_n|}\\
&\qquad\times\sum_{\substack{(t_i,t_{i-1},j_i,l_i)\\ \in\mathcal{T}_n^2\times\mathcal{J}_n\times\mathcal{L}_n}}\mathsf{E}\left[\hat{e}_i^{(n)}(j_i|\phi_n(t_{i-1}),t_i,l_i)\right].
\end{aligned}\right\} \quad (83)$$

By the symmetrical property of random coding it suffices to evaluate $\mathsf{E}[\tilde{e}_i^{(n)}\ (1|\phi_n(\ t_{i-1}),1,1)]$ and $\mathsf{E}[\hat{e}_i^{(n)}\ (1|\phi_n(\ t_{i-1}),1,1)]$. In a manner quite similar to that of the derivation of the upper bound of $\mathsf{E}[\tilde{e}_{2,i}^{(n)}\ (1|\phi_n(t_{i-1})\ ,1,1)]$ and $\mathsf{E}[\tilde{e}_{2,i}^{(n)}\ (1|\phi_n(t_{i-1}))]$, we obtain

$$\begin{aligned}
&\mathsf{E}[\tilde{e}_i^{(n)}(1|\phi_n(t_{i-1}),1,1)]\\
&=\Pr\left\{(S^n,U^n,X^n,Z^n)\notin\mathcal{A}_{XZ|US,\epsilon}\right\}\\
&\mathsf{E}[\hat{e}_i^{(n)}(1|\phi_n(t_{i-1}),1,1)]\le 2^{-n\epsilon}.
\end{aligned}$$

Hence we have

$$\mathsf{E}\left[e_i^{(n)}\right]\le\Pr\left\{(S^n,U^n,X^n,Z^n)\notin\mathcal{A}_{XZ|US,\epsilon}\right\}+2^{-n\epsilon}.$$

By an argument quite similar to that of the derivation of (70), we can prove the formulas of $\mathsf{E}\left[e_{ZX|S,i}^{(n)}\right]$ and $\mathsf{E}\left[e_{ZU|S,i}^{(n)}\right]$ stated in Lemma 2. We omit the proofs. ■

B. Proofs of Lemmas 3 and 11

Proof of Lemma 3: On a lower bound of $H(L_{n,i}|L_n^{(i-1)} Z^{nB})$, we have the following chain of inequalities:

$$\begin{aligned}
&H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\
&\geq H(L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&= H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&\quad -H(J_{n,i}|L_{n,i}L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&\geq H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&\quad -H(J_{n,i}|Z_{ni+1}^{n(i+1)}W_{n,i}T_{n,i}L_{n,i}). \qquad (84)
\end{aligned}$$

By Fano's inequality, we have

$$\frac{1}{n}H(J_{n,i}|Z_{ni+1}^{n(i+1)}W_{n,i}T_{n,i}L_{n,i}) \leq r_2 e_i^{(n)} + \frac{1}{n}. \qquad (85)$$

From (84) and (85), we have

$$\begin{aligned}
&H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\
&\geq H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i}) - nr_2e_i^{(n)} - 1\,. \qquad (86)
\end{aligned}$$

On the first quantity in the right members of (86), we have the following chain of inequalities:

$$\begin{aligned}
&H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&= H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z_{[i]}^{nB}W_{n,i}T_{n,i})\\
&\quad -I(Z_{n(i-1)+1}^{ni};J_{n,i}L_{n,i}|L_n^{(i-1)}Z_{[i]}^{nB}W_{n,i}T_{n,i})\\
&= H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z_{[i]}^{nB}W_{n,i}T_{n,i})\\
&\quad +H(Z_{n(i-1)+1}^{ni}|Z_{[i]}^{nB}W_{n,i}T_{n,i}J_{n,i}L_n^{(i)})\\
&\quad -H(Z_{n(i-1)+1}^{ni}|Z_{[i]}^{nB}W_{n,i}T_{n,i}J_{n,i}L_n^{(i-1)})\\
&= \log\left(|\mathcal{J}_n|\,|\mathcal{L}_n|\right) + H(Z_{n(i-1)+1}^{ni}|Z_{[i]}^{nB}W_{n,i}T_{n,i}J_{n,i}L_n^{(i)})\\
&\quad -H(Z_{n(i-1)+1}^{ni}|L_n^{(i-1)}Z_{[i]}^{nB}W_{n,i}T_{n,i}J_{n,i})\\
&\geq n(r_1+r_2) - 2 + H(Z_{n(i-1)+1}^{ni}|Z_{[i]}^{nB}W_{n,i}T_{n,i}J_{n,i}L_n^{(i)})\\
&\quad -H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i})\\
&\overset{\text{(a)}}{=} n(r_1+r_2) + H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i}J_{n,i}L_{n,i})\\
&\quad -H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i}) - 2\,. \qquad (87)
\end{aligned}$$

Equality (a) follows from the following Markov chain:

$$Z_{n(i-1)+1}^{ni} \to W_{n,i}T_{n,i}J_{n,i}L_{n,i} \to Z_{[i]}^{nB}L_n^{(i-1)}\,.$$

To derive a lower bound of $H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i}J_{n,i},L_{n,i})$, set

$$\begin{aligned}
\mathcal{B}_1^* \stackrel{\triangle}{=} \{&(w,t,j,l,\boldsymbol{z}):\\
&(\boldsymbol{s}(w),\boldsymbol{x}(w,t,j,l),\boldsymbol{z}) \in \mathcal{B}_{Z|XS,\epsilon}\}\,.
\end{aligned}$$

By definition of $\mathcal{B}_1^*$, if $(w,t,j,l,\boldsymbol{z}) \in \mathcal{B}_1^*$, we have

$$-\frac{1}{n}\log p_{Z|XS}(\boldsymbol{z}|\boldsymbol{x}(w,t,j,l),\boldsymbol{s}(w)) \geq H(Z|XS) - \epsilon\,.$$

By definition of $e_{Z|XS,i}^{(n)}$, we have

$$\Pr\{(W_{n,i},T_{n,i},J_{n,i},L_{n,i},Z_{n(i-1)+1}^{ni}) \notin \mathcal{B}_1^*\} = e_{Z|XS,i}^{(n)}\,.$$

Then, we have

$$\begin{aligned}
&H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i}J_{n,i}L_{n,i})\\
&\geq n[H(Z|XS)-\epsilon]\\
&\quad \times \Pr\{(W_{n,i},T_{n,i},J_{n,i},L_{n,i},Z_{n(i-1)+1}^{ni}) \in \mathcal{B}_1^*\}\\
&\geq n[H(Z|XS)-\epsilon](1-e_{Z|XS,i}^{(n)})\\
&\geq n[H(Z|XS)-\epsilon] - nH(Z|XS)e_{Z|XS,i}^{(n)}\,. \qquad (88)
\end{aligned}$$

To derive an upper bound of $H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i})$, set

$$\mathcal{B}_2^* \stackrel{\triangle}{=} \left\{(w,t,\boldsymbol{z}) : (\boldsymbol{s}(w),\boldsymbol{u}(w,t),\boldsymbol{z}) \in \mathcal{B}_{Z|US,\epsilon}\right\}.$$

By definition of $\mathcal{B}_2^*$, if $(w,t,\boldsymbol{z}) \in \mathcal{B}_2^*$, we have

$$-\frac{1}{n}\log p_{Z|US}(\boldsymbol{z}|\boldsymbol{u}(w,t),\boldsymbol{s}(w)) \leq H(Z|US) + \epsilon\,.$$

By definition of $e_{Z|US,i}^{(n)}$, we have

$$\Pr\{(W_{n,i},T_{n,i},Z_{n(i-1)+1}^{ni}) \notin \mathcal{B}_2^*\} = e_{Z|US,i}^{(n)}\,.$$

Set

$$\mathcal{D} \stackrel{\triangle}{=} \{(w,t) : (w,t,\boldsymbol{z}) \in (\mathcal{B}_2^*)^c \text{ for some } \boldsymbol{z}\}$$

and for $(w,t) \in \mathcal{D}$, set

$$\mathcal{D}(w,t) \stackrel{\triangle}{=} \{\boldsymbol{z} : (w,t,\boldsymbol{z}) \in (\mathcal{B}_2^*)^c\}\,.$$

Then, we have

$$\begin{aligned}
&H(Z_{n(i-1)+1}^{ni}|W_{n,i}T_{n,i})\\
&\leq n[H(Z|US)+\epsilon] - \sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\\
&\quad \times \log p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)\,. \qquad (89)
\end{aligned}$$

We derive an upper bound of the second term in the right member of (89). Let $\bar{Z}$ be a random variable uniformly distributed on $\mathcal{Z}$. Let $\bar{Z}^n = (\bar{Z}_1,\bar{Z}_2,\cdots,\bar{Z}_n)$ be n independent copies of $\bar{Z}$. We assume that $\bar{Z}^n$ is independent of W_n and T_n. We first observe that

$$\begin{aligned}
&-\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log\frac{p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)}{p_{\bar{Z}^n}(\boldsymbol{z})}\\
&= \sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log\frac{p_{\bar{Z}^n}(\boldsymbol{z})}{p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)}\\
&\overset{\text{(a)}}{\leq} (\log\mathrm{e})\cdot\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\\
&\qquad \times\left[\frac{p_{\bar{Z}^n}(\boldsymbol{z})}{p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)} - 1\right]\\
&= (\log\mathrm{e})\cdot\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} [p_{\bar{Z}^n}(\boldsymbol{z})p_{W_nT_n}(w,t)\\
&\qquad -p_{Z^nW_nT_n}(\boldsymbol{z},w,t)]\\
&= (\log\mathrm{e})\cdot\left[p_{\bar{Z}^nW_nT_n}(\mathcal{B}_2^*) - p_{Z^nW_nT_n}(\mathcal{B}_2^*)\right] \leq \log\mathrm{e}\,. \qquad (90)
\end{aligned}$$

Step (a) follows from the inequality $\log a \leq (\log \mathrm{e})(a-1)$. From (90), we have

$$\begin{aligned}
&-\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)\\
&\leq -\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log p_{\bar{Z}^n}(\boldsymbol{z})+\log \mathrm{e}\\
&= n\sum_{(w,t)\in\mathcal{D}}\sum_{\boldsymbol{z}\in\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log|\mathcal{Z}|+\log \mathrm{e}\\
&= ne^{(n)}_{Z|US,i}\log|\mathcal{Z}|+\log \mathrm{e}\,. \qquad (91)
\end{aligned}$$

Combining (86)-(89) and (91), we have

$$\begin{aligned}
&\frac{1}{n}H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\
&\geq r_1+r_2-I(X;Z|US)-2\epsilon-\frac{3+\log \mathrm{e}}{n}\\
&\quad-\left[(\log|\mathcal{Z}|)e^{(n)}_{Z|US,i}+H(Z|XS)e^{(n)}_{Z|XS,i}\right],\\
&\geq r_1+r_2-I(X;Z|US)-2\epsilon-\frac{3+\log \mathrm{e}}{n}\\
&\quad-r_2e_i^{(n)}-(\log|\mathcal{Z}|)\left[e^{(n)}_{Z|US,i}+e^{(n)}_{Z|XS,i}\right],
\end{aligned}$$

completing the proof. ∎

Proof of Lemma 11: In a manner quite similar to the derivation of (86) and (87) in the proof of Lemma 3, we have

$$\begin{aligned}
&H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\
&\geq H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})-nr_2e_i^{(n)}-1, \qquad (92)\\
&H(J_{n,i}L_{n,i}|L_n^{(i-1)}Z^{nB}W_{n,i}T_{n,i})\\
&\geq n(r_1+r_2)+h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i}J_{n,i}L_{n,i})\\
&\quad-h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i})-2. \qquad (93)
\end{aligned}$$

On a lower bound of $h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i}J_{n,i}L_{n,i})$, we have

$$\begin{aligned}
&h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i}J_{n,i}L_{n,i})\\
&\geq n[h(Z|XS)-\epsilon]\\
&\quad\times\Pr\{(W_{n,i},T_{n,i},J_{n,i},L_{n,i},Z^{ni}_{n(i-1)+1})\in\mathcal{B}_1^*\}\\
&\geq n[h(Z|XS)-\epsilon](1-e^{(n)}_{Z|XS,i})\\
&\geq n[h(Z|XS)-\epsilon]-nh(Z|XS)e^{(n)}_{Z|XS,i}\\
&= n[h(Z|XS)-\epsilon]-n\left\{\tfrac{1}{2}\log(2\pi\mathrm{e}N_2)\right\}e^{(n)}_{Z|XS,i}\,. \qquad (94)
\end{aligned}$$

Next, we derive an upper bound of $h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i})$. By definition of $\mathcal{B}_2^*$, if $(w,t,\boldsymbol{z})\in\mathcal{B}_2^*$, we have

$$-\frac{1}{n}\log p_{Z|US}(\boldsymbol{z}|\boldsymbol{u}(w,t),\boldsymbol{s}(w))\leq h(Z|US)+\epsilon\,.$$

Then we have

$$\begin{aligned}
&h(Z^{ni}_{n(i-1)+1}|W_{n,i}T_{n,i})\\
&\leq n[h(Z|US)+\epsilon]-\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\\
&\quad\times\log p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)\mathrm{d}\boldsymbol{z}\,. \qquad (95)
\end{aligned}$$

We derive an upper bound of the second term in the right member of (95). Let $\bar{Z}$ be a random variable whose density function denoted by $p_{\bar{Z}}(z)$ is

$$p_{\bar{Z}}(z)=\frac{1}{2}\mathrm{e}^{-|z|}\,.$$

Let $\bar{Z}^n=(\bar{Z}_1,\bar{Z}_2,\cdots,\bar{Z}_n)$ be n independent copies of $\bar{Z}$. We assume that $\bar{Z}^n$ is independent of W_n and T_n. For $\boldsymbol{z}\stackrel{\triangle}{=}(z_1,z_2,\cdots,z_n)$, the density function $p_{\bar{Z}^n}(\boldsymbol{z})$ of $\bar{Z}^n$ is

$$p_{\bar{Z}^n}(\boldsymbol{z})=\left(\frac{1}{2}\right)^n\prod_{i=1}^n\mathrm{e}^{-|z_i|}\,.$$

In a manner quite similar to the derivation of (90) in the proof of Lemma 3, we have

$$\begin{aligned}
&-\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log\frac{p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)}{p_{\bar{Z}^n}(\boldsymbol{z})}\mathrm{d}\boldsymbol{z}\\
&\leq\log \mathrm{e}\,. \qquad (96)
\end{aligned}$$

From (96), we have

$$\begin{aligned}
&-\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log p_{Z^n|W_nT_n}(\boldsymbol{z}|w,t)\mathrm{d}\boldsymbol{z}\\
&\leq -\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\log p_{\bar{Z}^n}(\boldsymbol{z})\mathrm{d}\boldsymbol{z}+\log \mathrm{e}\\
&= n\left\{\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\mathrm{d}\boldsymbol{z}\right\}+\log \mathrm{e}\\
&\quad+\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\left\{\sum_{i=1}^n|z_i|\right\}\mathrm{d}\boldsymbol{z}\,. \qquad (97)
\end{aligned}$$

On the last term in (97), we have the following chain of inequalities:

$$\begin{aligned}
&\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\left\{\sum_{i=1}^n|z_i|\right\}\mathrm{d}\boldsymbol{z}\\
&\stackrel{(a)}{\leq}\sum_{(w,t)\in\mathcal{D}}\left\{\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&\quad\times\left\{\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\left\{\sum_{i=1}^n|z_i|\right\}^2\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&\stackrel{(b)}{\leq}\left\{\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&\quad\times\left\{\sum_{(w,t)\in\mathcal{D}}\int_{\mathcal{D}(w,t)} p_{Z^nW_nT_n}(\boldsymbol{z},w,t)\left\{\sum_{i=1}^n|z_i|\right\}^2\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&\leq\sqrt{e^{(n)}_{Z|US,i}}\left\{\int p_{Z^n}(\boldsymbol{z})\left\{\sum_{i=1}^n|z_i|\right\}^2\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&\stackrel{(c)}{\leq}\sqrt{e^{(n)}_{Z|US,i}}\left\{n\int p_{Z^n}(\boldsymbol{z})\left\{\sum_{i=1}^n|z_i|^2\right\}\mathrm{d}\boldsymbol{z}\right\}^{\frac{1}{2}}\\
&=\sqrt{e^{(n)}_{Z|US,i}}\left\{n\sum_{i=1}^n\int z_i^2p_{Z_i}(z_i)\mathrm{d}z_i\right\}^{\frac{1}{2}}. \qquad (98)
\end{aligned}$$

Steps (a)-(c) follow from the Cauchy-Schwarz inequality. On the other hand, we have

$$\begin{aligned}\sum_{i=1}^{n}\int z_i^2 p_{Z_i}(z_i)\mathrm{d}z_i &= \sum_{i=1}^{n}\mathbf{E}\left[|X_i+\xi_{2,i}|^2\right]\\ &= \sum_{i=1}^{n}\mathbf{E}\left[|X_i|^2\right]+\sum_{i=1}^{n}\mathbf{E}\left[|\xi_{2,i}|^2\right]\\ &\le n(P_1+N_2)\,. \end{aligned}\tag{99}$$

Combining (92)-(95) and (97)-(99), we have

$$\begin{aligned}&\frac{1}{n}H(L_{n,i}|L_n^{(i-1)}Z^{nB})\\ &\ge r_1+r_2-I(X;Z|US)-2\epsilon-\frac{3+\log\mathrm{e}}{n}\\ &\quad -r_2e_i^{(n)}-\left[e_{Z|US,i}^{(n)}+\sqrt{(P_1+N_2)e_{Z|US,i}^{(n)}}\right]\\ &\quad -\left\{\tfrac{1}{2}\log(2\pi\mathrm{e}N_2)\right\}e_{Z|XS,i}^{(n)}\,,\end{aligned}$$

completing the proof. ■

C. Proof of Lemma 4

Proof of Lemma 4: We first observe that we have the following chains of inequalities:

$$\begin{aligned}\log|\mathcal{M}_n| &= H(M_n)\\ &= I(M_n;Y^n)+H(M_n|Y^n) &(100)\\ &= I(M_n;Z^n)+H(M_n|Z^n)\,, &(101)\\ \log|\mathcal{K}_n| &= H(K_n)=H(K_n|M_n)\\ &= I(K_n;Y^n|M_n)+H(K_n|Y^nM_n)\,, &(102)\\ H(K_n|Z^n) &= H(K_n|Z^nM_n)+I(K_n;M_n|Z^n)\\ &= H(K_n|M_n)-I(K_n;Z^n|M_n)\\ &\quad +I(K_n;M_n|Z^n)\\ &= I(K_n;Y^n|M_n)-I(K_n;Z^n|M_n)\\ &\quad +H(K_n|Y^nM_n)+I(K_n;M_n|Z^n)\\ &\le I(K_n;Y^n|M_n)-I(K_n;Z^n|M_n)\\ &\quad +H(K_n|Y^nM_n)+H(M_n|Z^n)\,, &(103)\\ &\le \log|\mathcal{K}_n|-I(K_n;Z^n|M_n)\\ &\quad +H(K_n|Y^nM_n)+H(M_n|Z^n)\,. &(104)\end{aligned}$$

Here, we suppose that $(R_0,R_1,R_{\mathrm{e}})\in\mathcal{R}_{\mathrm{s}}^*(\Gamma)$. Set $\lambda^{(n)}\stackrel{\triangle}{=}\max\{\lambda_1^{(n)},\lambda_2^{(n)}\}$. Then, by Fano's inequality we have

$$\left.\begin{aligned}H(M_n|Y^n)&\le\log|\mathcal{M}_n|\,\lambda^{(n)}+1\\ H(M_n|Z^n)&\le\log|\mathcal{M}_n|\,\lambda^{(n)}+1\\ H(K_n|Y^nM_n)&\le\log|\mathcal{K}_n|\,\lambda^{(n)}+1\,.\end{aligned}\right\}\tag{105}$$

Set

$$\left.\begin{aligned}\tau_{1,n}&\stackrel{\triangle}{=}\tfrac{1}{n}\log|\mathcal{M}_n|\,\lambda^{(n)}+\tfrac{1}{n}\\ \tau_{2,n}&\stackrel{\triangle}{=}\tfrac{1}{n}\log|\mathcal{K}_n|\,\lambda^{(n)}+\tfrac{1}{n}\,.\end{aligned}\right\}$$

From (100)-(105), we have

$$\left.\begin{aligned}\tfrac{1}{n}\log|\mathcal{M}_n|&\le\tfrac{1}{n}\min\{I(M_n;Y^n),I(M_n;Z^n)\}+\tau_{1,n}\\ \tfrac{1}{n}\log|\mathcal{K}_n|&\le\tfrac{1}{n}I(K_n;Y^n|M_n)+\tau_{2,n}\\ \tfrac{1}{n}H(K_n|Z^n)&\le\tfrac{1}{n}\log|\mathcal{K}_n|-\tfrac{1}{n}I(K_n;Z^n|M_n)\\ &\quad+\tau_{1,n}+\tau_{2,n}\\ \tfrac{1}{n}H(K_n|Z^n)&\le\tfrac{1}{n}I(K_n;Y^n|M_n)-\tfrac{1}{n}I(K_n;Z^n|M_n)\\ &\quad+\tau_{1,n}+\tau_{2,n}.\end{aligned}\right\}\tag{106}$$

Set

$$\left.\begin{aligned}\delta_{1,n}&\stackrel{\triangle}{=}\tau_{1,n}+\left[R_0-\tfrac{1}{n}\log|\mathcal{M}_n|\right]^+\\ \delta_{2,n}&\stackrel{\triangle}{=}\tau_{2,n}+\left[R_1-\tfrac{1}{n}\log|\mathcal{K}_n|\right]^+\\ \delta_{3,n}&\stackrel{\triangle}{=}\tau_{1,n}+\tau_{2,n}+\left[R_{\mathrm{e}}-\tfrac{1}{n}H(K_n|Z^n)\right]^+\\ &\quad+\left[\tfrac{1}{n}\log|\mathcal{K}_n|-R_1\right]^+\\ \delta_{4,n}&\stackrel{\triangle}{=}\tau_{1,n}+\tau_{2,n}+\left[R_{\mathrm{e}}-\tfrac{1}{n}H(K_n|Z^n)\right]^+\,.\end{aligned}\right\}\tag{107}$$

It is obvious that when $(R_0,R_1,R_{\mathrm{e}})\in\mathcal{R}_{\mathrm{s}}^*(\Gamma)$, the above $\delta_{i,n}$, $i=1,2,3,4$ tend to zero as $n\to\infty$. From (106) and (107), we have (21) for $(R_0,R_1,R_{\mathrm{e}})\in\mathcal{R}_{\mathrm{s}}^*(\Gamma)$. ■

D. Proof of Lemma 6

Proof of Lemma 6: We first prove (23) and (24). We have the following chains of inequalities:

$$\begin{aligned}&I(M_n;Y^n)=H(Y^n)-H(Y^n|M_n)\\ &=\sum_{i=1}^{n}\left\{H(Y_i|Y^{i-1})-H(Y_i|Y^{i-1}M_n)\right\}\\ &\le\sum_{i=1}^{n}\left\{H(Y_i)-H(Y_i|Y^{i-1}Z^{i-1}S_iM_n)\right\}\\ &=\sum_{i=1}^{n}I(U_iS_i;Y_i)\,,\\ &I(M_n;Z^n)=H(M_n)-H(M_n|Z^n)\\ &=\sum_{i=1}^{n}\left\{H(M_n|Z^{i-1})-H(M_n|Z^i)\right\}\\ &\overset{(a)}{=}\sum_{i=1}^{n}\left\{H(M_n|Z^{i-1}S_i)-H(M_n|Z^i)\right\}\\ &\le\sum_{i=1}^{n}\left\{H(M_n|Z^{i-1}S_i)-H(M_n|Z^iS_i)\right\}\\ &=\sum_{i=1}^{n}I(M_n;Z_i|Z^{i-1}S_i)\\ &=\sum_{i=1}^{n}\left\{H(Z_i|Z^{i-1}S_i)-H(Z_i|Z^{i-1}S_iM_n)\right\} &(108)\\ &\le\sum_{i=1}^{n}\left\{H(Z_i|S_i)-H(Z_i|Y^{i-1}Z^{i-1}S_iM_n)\right\}\\ &=\sum_{i=1}^{n}I(U_i;Z_i|S_i)\,.\end{aligned}$$

Step (a) follows from $S_i\to M_n\to Z^{i-1}$. Next, we prove

(25). We have the following chain of inequalities:

$$
\begin{aligned}
I(K_nM_n;Y^n) &\overset{(a)}{\leq} I(X^n;Y^n) = \sum_{i=1}^{n} I(Y_i;X^n|Y^{i-1}) \\
&= \sum_{i=1}^{n} \big\{H(Y_i|Y^{i-1}) - H(Y_i|Y^{i-1}X^n)\big\} \\
&\leq \sum_{i=1}^{n} \big\{H(Y_i) - H(Y_i|Y^{i-1}X^nS_i)\big\} \\
&\overset{(b)}{=} \sum_{i=1}^{n} \{H(Y_i) - H(Y_i|X_iS_i)\} = \sum_{i=1}^{n} I(X_iS_i;Y_i)
\end{aligned}
$$

Step (a) follows from $Y^n \to X^n \to K_nM_n$. Step (b) follows from $Y_i \to X_iS_i \to Y^{i-1}X_{[i]}$. Thirdly, we prove (26). We have the following chain of inequalities:

$$
\begin{aligned}
& I(K_n;Y^n|M_n) \leq I(K_n;Y^nZ^n|M_n) \\
&= I(K_nM_n;Y^nZ^n|M_n) \overset{(a)}{\leq} I(X^n;Y^nZ^n|M_n) \\
&= H(X^n|M_n) - H(X^n|Y^nZ^nM_n) \\
&= \sum_{i=1}^{n} \big\{H(X^n|Y^{i-1}Z^{i-1}M_n) - H(X^n|Y^iZ^iM_n)\big\} \\
&\overset{(b)}{=} \sum_{i=1}^{n} \big\{H(X^n|Y^{i-1}Z^{i-1}M_nS_i) - H(X^n|Y^iZ^iM_n)\big\} \\
&\leq \sum_{i=1}^{n} \big\{H(X^n|Y^{i-1}Z^{i-1}M_nS_i) - H(X^n|Y^iZ^iM_nS_i)\big\} \\
&= \sum_{i=1}^{n} I(X^n;Y_iZ_i|U_iS_i) \\
&= \sum_{i=1}^{n} \{H(Y_iZ_i|U_iS_i) - H(Y_iZ_i|U_iS_iX^n)\} \\
&\overset{(c)}{=} \sum_{i=1}^{n} \{H(Y_iZ_i|U_iS_i) - H(Y_iZ_i|X_iS_i)\} \\
&= \sum_{i=1}^{n} I(X_i;Y_iZ_i|U_iS_i)\,.
\end{aligned}
$$

Step (a) follows from the Markov chain $Y^nZ^n \to X^n \to K_nM_n$. Step (b) follows from $S_i \to Z^{i-1} \to X^nY^{i-1}M_n$. Step (c) follows from $Y_iZ_i \to X_iS_i \to U_iX_{[i]}$. Fourthly, we prove (27). We have the following chain of inequalities:

$$
\begin{aligned}
& I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n) \\
&\leq I(K_n;Y^nZ^n|M_n) - I(K_n;Z^n|M_n) \\
&= I(K_n;Y^n|Z^nM_n) = I(K_nM_n;Y^n|Z^nM_n) \\
&\overset{(a)}{\leq} I(X^n;Y^n|Z_nM_n) \\
&= H(Y^n|Z^nM_n) - H(Y^n|Z^nX^nK_nM_n) \\
&= \sum_{i=1}^{n} \big\{H(Y_i|Y^{i-1}Z^nM_n) - H(Y_i|Y^{i-1}Z^nX^n)\big\} \\
&\leq \sum_{i=1}^{n} \big\{H(Y_i|Y^{i-1}Z^iM_n) - H(Y_i|Y^{i-1}Z^nS_iX^n)\big\} \\
&\overset{(b)}{=} \sum_{i=1}^{n} \big\{H(Y_i|Y^{i-1}Z^iS_iM_n) - H(Y_i|Y^{i-1}Z^nS_iX^n)\big\} \\
&= \sum_{i=1}^{n} \{H(Y_i|U_iS_iZ_i) - H(Y_i|U_iS_iZ^nS_iX^n)\} \\
&\overset{(c)}{=} \sum_{i=1}^{n} \{H(Y_i|U_iS_iZ_i) - H(Y_i|U_iS_iZ_iX_i)\} \\
&= \sum_{i=1}^{n} I(X_i;Y_i|Z_iU_iS_i)\,.
\end{aligned}
$$

Step (a) follows from the Markov chain $Y^nZ^n \to X^n \to K_nM_n$. Step (b) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$
S_i \to Z^{i-1} \to Y^iZ^iK_nM_n\,. \tag{109}
$$

Step (b) follows from the above Markov chain. Step (c) follows from $Y_i \to Z_iX_iS_i \to Y^{i-1}Z_{[i]}X_{[i]}$. Finally, we prove (28). We have the following chain of inequalities:

$$
\begin{aligned}
& I(K_n;Z^n|M_n) = H(Z^n|M_n) - H(Z^n|K_nM_n) \\
&\overset{(a)}{=} H(Z^n|M_n) - H(Z^n|X^n) \\
&= \sum_{i=1}^{n} \big\{H(Z_i|Z^{i-1}M_n) - H(Z_i|Z^{i-1}X^n)\big\} \\
&\overset{(b)}{=} \sum_{i=1}^{n} \big\{H(Z_i|Z^{i-1}S_iM_n) - H(Z_i|Z^{i-1}S_iX^n)\big\} \\
&\geq \sum_{i=1}^{n} \{H(Z_i|U_iS_i) - H(Z_i|X_iS_i)\} \\
&\overset{(c)}{=} \sum_{i=1}^{n} \{H(Z_i|U_iS_i) - H(Z_i|X_iS_iU_i)\} \\
&= \sum_{i=1}^{n} I(X_i;Z_i|U_iS_i)\,.
\end{aligned}
$$

Step (a) follows from that f_n is a one-to-one mapping. Step (b) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$
S_i \to Z^{i-1} \to Z_iM_nX^n\,. \tag{110}
$$

Step (b) follows from the above Markov chain. Step (c) follows from $Z_i \to X_iS_i \to U_i$. Thus, the proof of Lemma 6 is completed. ■

E. Proofs of Lemmas 8 and 10

In this appendix we prove Lemmas 8 and 10. We first present a lemma necessary to prove those lemmas.

Lemma 13:

$$I(M_n;Y^n) \le \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} S_i M_n; Y_i)\,, \qquad (111)$$

$$I(M_n;Z^n) \le \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} M_n; Z_i|S_i)\,, \qquad (112)$$

$$I(K_nM_n;Y^n) \le \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} S_i K_n M_n; Y_i)\,, \quad (113)$$

$$I(K_nM_n;Z^n) \le \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} K_n M_n; Z_i|S_i)\,, (114)$$

$$\begin{aligned} &I(Y^n;K_n|M_n) - I(Z^n;K_n|M_n) \\ &= \sum_{i=1}^{n} \big\{ I(K_n;Y_i|Y_{i+1}^n Z^{i-1} M_n S_i) \\ &\qquad - I(K_n;Z_i|Y_{i+1}^n Z^{i-1} M_n S_i) \big\}\,. \end{aligned} \qquad (115)$$

Proof: We first prove (111) and (112). We have the following chains of inequalities:

$$\begin{aligned} I(M_n;Y^n) &= \sum_{i=1}^{n} \big\{ H(Y_i|Y_{i+1}^n) - H(Y_i|Y_{i+1}^n M_n) \big\} \\ &\le \sum_{i=1}^{n} \big\{ H(Y_i) - H(Y_i|Y_{i+1}^n Z^{i-1} S_i M_n) \big\} \\ &= \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} S_i M_n; Y_i), \\ I(M_n;Z^n) &\overset{(a)}{\le} \sum_{i=1}^{n} \big\{ H(Z_i|Z^{i-1} S_i) - H(Z_i|Z^{i-1} S_i M_n) \big\} \\ &\le \sum_{i=1}^{n} \big\{ H(Z_i|S_i) - H(Z_i|Y_{i+1}^n Z^{i-1} S_i M_n) \big\} \\ &= \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} M_n; Z_i|S_i)\,. \end{aligned}$$

Step (a) follows from (108). Next, we prove (113) and (114). We have the following chains of inequalities:

$$\begin{aligned} &I(K_nM_n;Y^n) = H(Y^n) - H(Y^n|K_nM_n) \\ &= \sum_{i=1}^{n} \big\{ H(Y_i|Y_{i+1}^n) - H(Y_i|Y_{i+1}^n K_n M_n) \big\} \\ &\le \sum_{i=1}^{n} \big\{ H(Y_i) - H(Y_i|Y_{i+1}^n Z^{i-1} S_i K_n M_n) \big\} \\ &= \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} S_i K_n M_n; Y_i)\,, \\ &I(K_nM_n;Z^n) \\ &= H(K_nM_n|Z^n) - H(K_nM_n|Z^n) \\ &= \sum_{i=1}^{n} \big\{ H(K_nM_n|Z^{i-1}) - H(K_nM_n|Z^i) \big\} \\ &\le \sum_{i=1}^{n} \big\{ H(K_nM_n|Z^{i-1}) - H(K_nM_n|Z^i S_i) \big\} \\ &\overset{(a)}{=} \sum_{i=1}^{n} \big\{ H(K_nM_n|Z^{i-1} S_i) - H(K_nM_n|Z^i S_i) \big\} \\ &= \sum_{i=1}^{n} I(K_nM_n; Z_i|Z^{i-1} S_i) \\ &= \sum_{i=1}^{n} \big\{ H(Z_i|Z^{i-1} S_i) - H(Z_i|Z^{i-1} S_i K_n M_n) \big\} \\ &\le \sum_{i=1}^{n} \big\{ H(Z_i|S_i) - H(Z_i|Y_{i+1}^n Z^{i-1} S_i K_n M_n) \big\} \\ &= \sum_{i=1}^{n} I(Y_{i+1}^n Z^{i-1} K_n M_n; Z_i|S_i)\,. \end{aligned}$$

Step (a) follows from $S_i \to Z^{i-1} \to K_nM_n$. Finally, we prove (115). We first observe the following two identities:

$$\begin{aligned} &H(Y^n|M_n) - H(Z^n|M_n) \\ &= \sum_{i=1}^{n} \big\{ H(Y_i|Y_{i+1}^n Z^{i-1} M_n) - H(Z_i|Y_{i+1}^n Z^{i-1} M_n) \big\}\,, \end{aligned} \qquad (116)$$

$$\begin{aligned} &H(Y^n|K_nM_n) - H(Z^n|K_nM_n) \\ &= \sum_{i=1}^{n} \big\{ H(Y_i|Y_{i+1}^n Z^{i-1} K_n M_n) \\ &\qquad - H(Z_i|Y_{i+1}^n Z^{i-1} K_n M_n) \big\}\,. \end{aligned} \qquad (117)$$

Those identities follow from an elementary computation based on the chain rule of entropy. Subtracting (117) from (116), we have

$$\begin{aligned} &I(Y^n;K_n|M_n) - I(Z^n;K_n|M_n) \\ &= \sum_{i=1}^{n} \big\{ I(K_n;Y_i|Y_{i+1}^n Z^{i-1} M_n) \\ &\qquad - I(K_n;Z_i|Y_{i+1}^n Z^{i-1} M_n) \big\} \\ &= \sum_{i=1}^{n} \big\{ -H(K_n|Y_i^n Z^{i-1} M_n) + H(K_n|Y_{i+1}^n Z^i M_n) \big\} \\ &\le \sum_{i=1}^{n} \big\{ -H(K_n|Y_i^n Z^{i-1} M_n S_i) + H(K_n|Y_{i+1}^n Z^i M_n) \big\} \\ &\overset{(a)}{=} \sum_{i=1}^{n} \big\{ -H(K_n;|Y_i^n Z^{i-1} M_n S_i) + H(K_n|Y_{i+1}^n Z^i M_n S_i) \big\} \\ &= \sum_{i=1}^{n} \big\{ I(K_n;Y_i|Y_{i+1}^n Z^{i-1} M_n S_i) \\ &\qquad - I(K_n;Z_i|Y_{i+1}^n Z^{i-1} M_n S_i) \big\}\,. \end{aligned}$$

Step (a) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$S_i \to Z^{i-1} \to Z_i Y_{i+1}^n K_n M_n. \qquad (118)$$

Step (a) follows from the above Markov chain. ■

Next, we present a lemma necessary to prove Lemma 8.

Lemma 14: For any sequence $\{U_i\}_{i=1}^n$ of random variables, we have

$$I(K_nM_n;Y^n) \le \sum_{i=1}^{n} I(X_i U_i S_i; Y_i)\,, \qquad (119)$$

$$I(K_nM_n;Z^n) \le \sum_{i=1}^{n} I(X_i U_i; Z_i|S_i)\,. \qquad (120)$$

Proof: We first prove (119). We have the following chain of inequalities:

$$\begin{aligned}
&I(K_nM_n;Y^n) \overset{\text{(a)}}{\leq} I(X^n;Y^n) = H(Y^n) - H(Y^n|X^n)\\
&= \sum_{i=1}^{n} \big\{H(Y_i|Y^{i-1}) - H(Y_i|Y^{i-1}X^n)\big\}\\
&\leq \sum_{i=1}^{n} \big\{H(Y_i) - H(Y_i|Y^{i-1}X^nS_i)\big\}\\
&\overset{\text{(b)}}{=} \sum_{i=1}^{n} \{H(Y_i) - H(Y_i|X_iS_i)\}\\
&\leq \sum_{i=1}^{n} \{H(Y_i) - H(Y_i|X_iU_iS_i)\} = \sum_{i=1}^{n} I(X_iU_iS_i;Y_i)\,.
\end{aligned}$$

Step (a) follows from the Markov chain $Y^n \to X^n \to K_nM_n$. Step (b) follows from $Y_i \to X_iS_i \to Y^{i-1}X_{[i]}$. Next, we prove (120). We have the following chain of inequalities:

$$\begin{aligned}
&I(K_nM_n;Z^n) \overset{\text{(a)}}{\leq} I(X^n;Z^n) = H(X^n) - H(X^n|Z^n)\\
&= \sum_{i=1}^{n} \big\{H(X^n|Z^{i-1}) - H(X^n|Z^i)\big\}\\
&\leq \sum_{i=1}^{n} \big\{H(X^n|Z^{i-1}) - H(X^n|Z^iS_i)\big\}\\
&\overset{\text{(b)}}{=} \sum_{i=1}^{n} \big\{H(X^n|Z^{i-1}S_i) - H(X^n|Z^iS_i)\big\}\\
&= \sum_{i=1}^{n} I(X^n;Z^i|Z^{i-1}S_i)\\
&= \sum_{i=1}^{n} \big\{H(Z_i|Z^{i-1}S_i) - H(Z_i|Z^iX^nS_i)\big\}\\
&\overset{\text{(c)}}{=} \sum_{i=1}^{n} \{H(Z_i|S_i) - H(Z_i|X_iS_i)\}\\
&\leq \sum_{i=1}^{n} \{H(Z_i|S_i) - H(Z_i|X_iU_iS_i)\} = \sum_{i=1}^{n} I(X_iU_i;Z_i|S_i)\,.
\end{aligned}$$

Step (a) follows from the Markov chain $Z^n \to X^n \to K_nM_n$. Step (b) follows from $S_i \to Z^{i-1} \to X^n$. Step (c) follows from $Z_i \to X_iS_i \to Z^{i-1}X_{[i]}$. Thus, the proof of Lemma 14 is completed. ∎

Proof of Lemma 8: Set $U_i = Y_{i+1}^n Z^{i-1} M_n$. It can easily be verified that U_i, $X_iS_iZ_i$, Y_i form a Markov chain $U_i \to X_iS_iZ_i \to Y_i$ in this order. From (111), (112), and (115) in Lemma 13, we obtain

$$\begin{aligned}
I(M_n;Y^n) &\leq \sum_{i=1}^{n} I(U_iS_i;Y_i),\\
I(M_n;Z^n) &\leq \sum_{i=1}^{n} I(U_i;Z_i|S_i),
\end{aligned}$$

and

$$\begin{aligned}
&I(Y^n;K_n|M_n) - I(Z^n;K_n|M_n)\\
&\leq \sum_{i=1}^{n} \{I(K_n;Y_i|U_iS_i) - I(K_n;Z_i|U_iS_i)\}\,, \qquad (121)
\end{aligned}$$

respectively. From (119), (120) in Lemma 14, we obtain

$$\begin{aligned}
I(K_nM_n;Y^n) &\leq \sum_{i=1}^{n} I(X_iU_iS_i;Y_i),\\
I(K_nM_n;Z^n) &\leq \sum_{i=1}^{n} I(X_iU_i;Z_i|S_i),
\end{aligned}$$

respectively. It remains to evaluate an upper bound of

$$I(K_n;Y_i|U_iS_i) - I(K_n;Z_i|U_iS_i)\,.$$

We have the following chain of inequalities:

$$\begin{aligned}
&I(K_n;Y_i|U_iS_i) - I(K_n;Z_i|U_iS_i)\\
&= H(Y_i|U_iS_i) - H(Y_i|K_nM_nU_iS_i)\\
&\quad -H(Z_i|U_iS_i) + H(Z_i|K_nM_nU_iS_i)\\
&\overset{\text{(a)}}{=} H(Y_i|U_iS_i) - H(Y_i|X^nU_iS_i)\\
&\quad -H(Z_i|U_iS_i) + H(Z_i|X^nU_iS_i)\\
&= H(Y_i|U_iS_i)\\
&\quad -H(Y_i|Z_iX^nU_iS_i) - I(Y_i;Z_i|X^nU_iS_i)\\
&\quad -H(Z_i|U_iS_i)\\
&\quad +H(Z_i|Y_iX^nU_iS_i) + I(Y_i;Z_i|X^nU_iS_i)\\
&= H(Y_i|U_iS_i) - H(Y_i|Z_iX^nU_iS_i)\\
&\quad -H(Z_i|U_iS_i) + H(Z_i|Y_iX^nU_iS_i)\\
&\overset{\text{(b)}}{=} H(Y_i|U_iS_i) - H(Y_i|Z_iX_iS_i)\\
&\quad -H(Z_i|U_iS_i) + H(Z_i|Y_iX^nU_iS_i)\\
&\leq H(Y_i|U_iS_i) - H(Y_i|Z_iX_iU_iS_i)\\
&\quad -H(Z_i|U_iS_i) + H(Z_i|Y_iX_iU_iS_i)\\
&= I(Y_i;Z_iX_i|U_iS_i) - I(Z_i;Y_iX_i|U_iS_i)\\
&= I(X_i;Y_i|U_iS_i) - I(X_i;Z_i|U_iS_i)\,.
\end{aligned}$$

Step (a) follows from $X^n = f_n(K_n, M_n)$ and f_n is a one-to-one mapping. Step (b) follows from $Y_i \to Z_iX_iS_i \to U_iX_{[i]}$. Finally, we prove (38). We have the following chain of inequalities:

$$\begin{aligned}
&I(K_n;Z^n|M_n) = H(Z^n|M_n) - H(Z^n|K_nM_n)\\
&\overset{\text{(a)}}{=} H(Z^n|M_n) - H(Z^n|X^n)\\
&= \sum_{i=1}^{n} \big\{H(Z_i|Z^{i-1}M_n) - H(Z_i|Z^{i-1}X^n)\big\}\\
&\overset{\text{(b)}}{=} \sum_{i=1}^{n} \big\{H(Z_i|Z^{i-1}S_iM_n) - H(Z_i|Z^{i-1}S_iX^n)\big\}\\
&\geq \sum_{i=1}^{n} \{H(Z_i|U_iS_i) - H(Z_i|X_iS_i)\}\\
&= \sum_{i=1}^{n} \{I(X_i;Z_i|U_iS_i) - I(U_i;Z_i|X_iS_i)\}\,.
\end{aligned}$$

Step (a) follows from that f_n is a one-to-one mapping. Step (b) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$S_i \to Z^{i-1} \to Z_iM_nX^n. \qquad (122)$$

Step (b) follows from the above Markov chain. ■

Proof of Lemma 10: This lemma immediately follows from Lemma 13. ■

F. Proof of Lemma 9

In this appendix we prove Lemma 9.

Proof of Lemma 9: Set $U_i \stackrel{\triangle}{=} Y^{i-1}Z_{i+1}^n M_n$. It can easily be verified that U_i, $X_iS_iZ_i$, Y_i form a Markov chain $U_i \to X_iS_iZ_i \to Y_i$ in this order. In a manner similar to the proof of Lemma 13, we obtain the following chains of inequalities:

$$\begin{aligned}
I(M_n;Y^n) &= \sum_{i=1}^n \big\{H(Y_i|Y^{i-1}) - H(Y_i|Y^{i-1}M_n)\big\} \\
&\le \sum_{i=1}^n \big\{H(Y_i) - H(Y_i|Y^{i-1}Z_{i+1}^n M_n)\big\} \\
&= \sum_{i=1}^n I(Y^{i-1}Z_{i+1}^n M_n; Y_i), \\
I(M_n;Z^n) &= H(Z^n) - H(Z^n|M_n) \\
&= \sum_{i=1}^n H(Z_i|Z^{i-1}) - \sum_{i=1}^n H(Z_i|Z_{i+1}^n M_n) \\
&\stackrel{(a)}{\le} \sum_{i=1}^n \big\{H(Z_i|S_i) - H(Z_i|Z_{i+1}^n M_n)\big\} \\
&\le \sum_{i=1}^n \big\{H(Z_i|S_i) - H(Z_i|Y^{i-1}Z_{i+1}^n S_i M_n)\big\} \\
&= \sum_{i=1}^n I(Y^{i-1}Z_{i+1}^n M_n; Z_i|S_i)\,.
\end{aligned}$$

Step (a) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$S_i \to Z^{i-1} \to Z_i M_n X^n. \tag{123}$$

Step (a) follows from the above Markov chain. Hence, we have

$$\begin{aligned}
I(M_n;Y^n) &\le \sum_{i=1}^n I(U_i;Y_i), \\
I(M_n;Z^n) &\le \sum_{i=1}^n I(U_i;Z_i|S_i).
\end{aligned}$$

Furthermore, by taking $\{U_i\}_{i=1}^n$ be constant in (119), (120) in Lemma 14, we obtain

$$\begin{aligned}
I(K_nM_n;Y^n) &\le \sum_{i=1}^n I(X_iS_i;Y_i), \\
I(K_nM_n;Z^n) &\le \sum_{i=1}^n I(X_i;Z_i|S_i),
\end{aligned}$$

respectively. It remains to evaluate an upper bound of

$$I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n)\,.$$

Since f_n is deterministic, we have

$$\begin{aligned}
&I(K_n;Y^n|M_n) - I(K_n;Z^n|M_n) \\
&= H(Y^n|M_n) - H(Z^n|M_n) - H(Y^n|X^n) \\
&\quad + H(Z^n|X^n)\,.
\end{aligned} \tag{124}$$

We separately evaluate the following two quantities:

$$H(Y^n|M_n) - H(Z^n|M_n), H(Y^n|X^n) - H(Z^n|X^n).$$

We observe the following two identities:

$$\begin{aligned}
&H(Y^n|M_n) - H(Z^n|M_n) \\
&= \sum_{i=1}^n \big\{H(Y_i|Y^{i-1}Z_{i+1}^n M_n) - H(Z_i|Y^{i-1}Z_{i+1}^n M_n)\big\}\,, \qquad (125) \\
&\quad -H(Y^n|X^n) + H(Z^n|X^n) \\
&= \sum_{i=1}^n \big\{-H(Y_i|Y_{i+1}^n Z^{i-1}X^n) + H(Z_i|Y_{i+1}^n Z^{i-1}X^n)\big\}\,. \qquad (126)
\end{aligned}$$

Those identities follow from an elementary computation based on the chain rule of entropy. From (125), we have

$$\begin{aligned}
&H(Y^n|M_n) - H(Z^n|M_n) \\
&= \sum_{i=1}^n \{H(Y_i|U_i) - H(Z_i|U_i)\}\,.
\end{aligned} \tag{127}$$

Next, we evaluate an upper bound of

$$-H(Y_i|Y_{i+1}^n Z^{i-1}X^n) + H(Z_i|Y_{i+1}^n Z^{i-1}X^n)\,.$$

Set $\tilde{U}_i \stackrel{\triangle}{=} Y_{i+1}^n Z^{i-1}X_{[i]}$. We have the following chain of inequalities:

$$\begin{aligned}
&-H(Y_i|Y_{i+1}^n Z^{i-1}X^n) + H(Z_i|Y_{i+1}^n Z^{i-1}X^n) \\
&= -H(Y_i|X_i\tilde{U}_i) + H(Z_i|X_i\tilde{U}_i) \\
&\le -H(Y_i|X_iS_i\tilde{U}_i) + H(Z_i|X_i\tilde{U}_i) \qquad (128) \\
&\stackrel{(a)}{=} -H(Y_i|X_iS_i\tilde{U}_i) + H(Z_i|X_iS_i\tilde{U}_i) \\
&= -H(Y_i|Z_iX_iS_i\tilde{U}_i) + I(Y_i;Z_i|X_iS_i\tilde{U}_i) \\
&\quad + H(Z_i|Y_iX_iS_i\tilde{U}_i) - I(Y_i;Z_i|X_iS_i\tilde{U}_i) \\
&= -H(Y_i|Z_iX_iS_i\tilde{U}_i) + H(Z_i|Y_iX_iS_i\tilde{U}_i) \\
&\stackrel{(b)}{=} -H(Y_i|Z_iX_iS_i) + H(Z_i|Y_iX_iS_i\tilde{U}_i) \\
&\le -H(Y_i|Z_iX_iS_i) + H(Z_i|Y_iX_iS_i) \\
&= -H(Y_i|X_iS_i) + I(Y_i;Z_i|X_iS_i) \\
&\quad + H(Z_i|X_iS_i) - I(Y_i;Z_i|X_iS_i) \\
&= -H(Y_i|X_iS_i) + H(Z_i|X_iS_i)\,. \qquad (129)
\end{aligned}$$

Step (a) follows from that $S_i = g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$S_i \to Z^{i-1} \to Z_i Y_{i+1}^n X^n. \tag{130}$$

Step (a) follows from the above Markov chain. Step (b) follows from $Y_i \to Z_iX_iS_i \to \tilde{U}_i$. Combining (124), (126), (127), and

(129), we obtain

$$\begin{aligned}
&I(K_n;Y^n|M_n)-I(K_n;Z^n|M_n)\\
&\le \sum_{i=1}^n\{H(Y_i|U_i)-H(Z_i|U_i)\\
&\qquad -H(Y_i|X_iS_i)+H(Z_i|X_iS_i)\}\\
&\le \sum_{i=1}^n\{H(Y_i|U_i)-H(Z_i|U_i)\\
&\qquad -H(Y_i|X_iS_iU_i)+H(Z_i|X_iS_i)\}\\
&= \sum_{i=1}^n\{I(X_iS_i;Y_i|U_i)-I(X_iS_i;Z_i|U_i)\\
&\qquad +I(U_i;Z_i|X_iS_i)\}\\
&= \sum_{i=1}^n\{I(X_i;Y_i|U_iS_i)-I(X_i;Z_i|U_iS_i)\\
&\qquad +\zeta(S_i;Y_i,Z_i|U_i)+I(U_i;Z_i|X_iS_i)\}\,.
\end{aligned}$$

Finally, we prove (46). We have the following chain of inequalities:

$$\begin{aligned}
&I(K_n;Z^n|M_n)=H(Z^n|M_n)-H(Z^n|K_nM_n)\\
&\overset{(a)}{=} H(Z^n|M_n)-H(Z^n|X^n)\\
&= \sum_{i=1}^n\left\{H(Z_i|Z_{i+1}^nM_n)-H(Z_i|Z^{i-1}X^n)\right\}\\
&\overset{(b)}{=} \sum_{i=1}^n\left\{H(Z_i|Z_{i+1}^nM_n)-H(Z_i|Z^{i-1}S_iX^n)\right\}\\
&\ge \sum_{i=1}^n\{H(Z_i|U_iS_i)-H(Z_i|X_iS_i)\}\\
&= \sum_{i=1}^n\{I(X_i;Z_i|U_iS_i)-I(U_i;Z_i|X_iS_i)\}\,.
\end{aligned}$$

Step (a) follows from that f_n is a one-to-one mapping. Step (b) follows from that $S_i=g_i(Z^{i-1})$ is a function of Z^{i-1} in the case where $\{g_i\}_{i=1}^n$ is restricted to be deterministic. In the case where $\{g_i\}_{i=1}^n$ is allowed to be stochastic, if Γ belongs to the class NL, we have the following Markov chain:

$$S_i\to Z^{i-1}\to Z_iX^n. \tag{131}$$

Step (b) follows from the above Markov chain. Thus, the proof of Lemma 9 is completed. ∎

G. Proof of Lemma 12

We first observe that by the Cauchy-Schwarz inequality we have

$$\begin{aligned}
\mathbf{E}_S\left(\mathbf{E}_{X(S)}X(S)\right)^2 &\le \mathbf{E}_S\left[\left(\sqrt{\mathbf{E}_{X(S)}X^2(S)}\sqrt{\mathbf{E}_{X(S)}1}\right)^2\right]\\
&=\mathbf{E}_S\mathbf{E}_{X(S)}X^2(S)\le P_1\,.
\end{aligned}$$

Then, there exits $\alpha\in[0,1]$ such that

$$\mathbf{E}_S\left(\mathbf{E}_{X(S)}X(S)\right)^2=\bar{\alpha}P_1\,.$$

We derive an upper bound of $h(Y)$. We have the following chain of inequalities:

$$\begin{aligned}
&h(Y)=h(X+S+\xi_1)\\
&\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\mathbf{E}_{XS}|X+S|^2+N_1\right)\right\}\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\mathbf{E}_XX^2+2\mathbf{E}_{XS}XS+\mathbf{E}_SS^2+N_1\right)\right\}\\
&\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(P_1+P_2+2\mathbf{E}_{XS}XS+N_1\right)\right\}\,. \qquad (132)
\end{aligned}$$

By the Cauchy-Schwarz inequality we have

$$\begin{aligned}
&\mathbf{E}_{XS}XS=\mathbf{E}_S\left[S\mathbf{E}_{X(S)}X(S)\right]\\
&\le \sqrt{\mathbf{E}_SS^2}\sqrt{\mathbf{E}_S\left(\mathbf{E}_{X(S)}X(S)\right)^2}=\sqrt{P_2}\sqrt{\bar{\alpha}P_1}\,. \qquad (133)
\end{aligned}$$

From (132) and (133), we have

$$h(Y)\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(P_1+P_2+\sqrt{\bar{\alpha}P_1P_2}+N_1\right)\right\}\,.$$

Next, we estimate an upper bound of $h(Y|S)$. We have the following chain of inequalities:

$$\begin{aligned}
&h(Y|S)=\mathbf{E}_S\left[h(X(S)+\xi_1)\right]\\
&\le \mathbf{E}_S\left[\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\mathbf{V}_{X(S)}\left[X(S)\right]+N_1\right)\right\}\right]\\
&= \mathbf{E}_S\Big[\tfrac{1}{2}\log\Big\{(2\pi\mathrm{e})\Big(\mathbf{E}_{X(S)}[X^2(S)]\\
&\qquad -\left(\mathbf{E}_{X(S)}X(S)\right)^2+N_1\Big)\Big\}\Big]\\
&\le \tfrac{1}{2}\log\Big\{(2\pi\mathrm{e})\Big(\mathbf{E}_S\mathbf{E}_{X(S)}[X^2(S)]\\
&\qquad -\mathbf{E}_S\left(\mathbf{E}_{X(S)}X(S)\right)^2+N_1\Big)\Big\}\\
&\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\alpha P_1+N_1\right)\right\}\,.
\end{aligned}$$

Similarly, we obtain

$$\begin{aligned}
&h(Z|S)\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\alpha P_1+N_2\right)\right\}\,,\\
&h(\tilde{Y}|S)\le \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\alpha P_1+\tilde{N}_1\right)\right\}\,. \qquad (134)
\end{aligned}$$

Since

$$h(\tilde{Y}|S)\ge h(\tilde{Y}|XS)=\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\tilde{N}_1\right\}$$

and (134), there exists $\beta\in[0,1]$ such that

$$h(\tilde{Y}|US)=\tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1+\tilde{N}_1\right)\right\}\,.$$

Finally, we derive lower bounds of $h(Y|US)$ and $h(Z|US)$. Let $\tilde{Y}(u,s)$ be a random variable with a conditional distribution of $\tilde{Y}$ for given $(U,S)=(u,s)$. Similar notations are used for Y and Z. From the relation (57) between X,S,Y,Z, and $\tilde{Y}$, we have

$$\begin{aligned}
Y(u,s)&=\tilde{Y}(u,s)+\bar{a}(s+\tilde{\xi}_2)\,, &(135)\\
Z(u,s)&=\tilde{Y}(u,s)-a(s+\tilde{\xi}_2)\,. &(136)
\end{aligned}$$

Note that $\tilde{Y}(u,s)$ is independent of $\tilde{\xi}_2$. Applying entropy power inequality to (135) and (136), we have

$$\begin{aligned}
\tfrac{1}{2\pi\mathrm{e}}2^{2h(Y(u,s))}&\ge \tfrac{1}{2\pi\mathrm{e}}2^{2h(\tilde{Y}(u,s))}+\tfrac{1}{2\pi\mathrm{e}}2^{2h\left(\bar{a}(s+\tilde{\xi}_2)\right)}\\
&=\tfrac{1}{2\pi\mathrm{e}}2^{2h(\tilde{Y}(u,s))}+\bar{a}^2\tilde{N}_2\,,\\
\tfrac{1}{2\pi\mathrm{e}}2^{2h(Z(u,s))}&\ge \tfrac{1}{2\pi\mathrm{e}}2^{2h(\tilde{Y}(u,s))}+\tfrac{1}{2\pi\mathrm{e}}2^{2h\left(a(s+\tilde{\xi}_2)\right)}\\
&=\tfrac{1}{2\pi\mathrm{e}}2^{2h(\tilde{Y}(u,s))}+a^2\tilde{N}_2\,,
\end{aligned}$$

from which we have

$$h(Y(u,s)) \geq F_1\left(h(\tilde{Y}(u,s))\right), \tag{137}$$

$$h(Z(u,s)) \geq F_2\left(h(\tilde{Y}(u,s))\right), \tag{138}$$

where

$$F_1(\gamma) \stackrel{\triangle}{=} \frac{1}{2}\log\left(2^{2\gamma} + (2\pi\mathrm{e})\bar{a}^2\tilde{N}_2\right),$$
$$F_2(\gamma) \stackrel{\triangle}{=} \frac{1}{2}\log\left(2^{2\gamma} + (2\pi\mathrm{e})a^2\tilde{N}_2\right).$$

By a simple computation we can show that $F_i(\gamma), i = 1, 2$ are monotone increasing and convex functions of γ. Taking the expectation of both sides of (137) with respect to (U, S), we have

$$\begin{aligned}
&h(Y|US)\\
&= \mathbf{E}_{US}\left[h(Y(U,S))\right] \geq \mathbf{E}_{US}\left[F_1\left(h(\tilde{Y}(U,S))\right)\right]\\
&\stackrel{(a)}{\geq} F_1\left(\mathbf{E}_{US}\left[h(\tilde{Y}(U,S))\right]\right) = F_1\left(h(\tilde{Y}|US)\right)\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + \tilde{N}_1 + \bar{a}^2\tilde{N}_2\right)\right\}\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + \tfrac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}\right.\right.\\
&\qquad\left.\left. + \tfrac{N_1^2+\rho^2N_1N_2-2\rho N_1\sqrt{N_1N_2}}{N_1+N_2-2\rho\sqrt{N_1N_2}}\right)\right\}\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + N_1\right)\right\}.
\end{aligned}$$

Step (a) follows from the convexity of $F_1(\gamma)$ and Jensen's inequality. Taking the expectation of both sides of (138) with respect to (U, S), we have

$$\begin{aligned}
&h(Z|US)\\
&= \mathbf{E}_{US}\left[h(Z(U,S))\right] \geq \mathbf{E}_{US}\left[F_2\left(h(\tilde{Y}(U,S))\right)\right]\\
&\stackrel{(a)}{\geq} F_2\left(\mathbf{E}_{US}\left[h(\tilde{Y}(U,S))\right]\right) = F_2\left(h(\tilde{Y}|US)\right)\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + \tilde{N}_1 + a^2\tilde{N}_2\right)\right\}\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + \tfrac{(1-\rho^2)N_1N_2}{N_1+N_2-2\rho\sqrt{N_1N_2}}\right.\right.\\
&\qquad\left.\left. + \tfrac{N_2^2+\rho^2N_1N_2-2\rho N_2\sqrt{N_1N_2}}{N_1+N_2-2\rho\sqrt{N_1N_2}}\right)\right\}\\
&= \tfrac{1}{2}\log\left\{(2\pi\mathrm{e})\left(\beta\alpha P_1 + N_2\right)\right\}.
\end{aligned}$$

Step (a) follows from the convexity of $F_2(\gamma)$ and Jensen's inequality. Thus, the proof of Lemma 12 is completed. ■

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Sys. Tech. Journal*, vol. 28, pp. 656-715, 1949.

[2] H. Yamamoto, "Coding theorems for Shannon cipher system with correlated source outputs and common information," *IEEE Trans. Inform. Theory*, vol. 40 pp. 85-95, 1994.

[3] ____, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inform. Theory*, vol. 43 pp. 827-835, 1997.

[4] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journal*, vol. 54, pp. 1355-1387, 1975.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 339-348, 1978.

[6] H. Yamamoto, "A source-coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Trans. Inform. Theory*, vol. 29, pp. 918-923, 1983.

[7] ____, "On secret sharing communication-systems with 2 or 3 channels," *IEEE Trans. Inform. Theory*, vol. 32, pp. 387-393, 1986.

[8] ____, "A rate-distortion problem for a communication-system with a secondary decoder to be hindered," *IEEE Trans. Inform. Theory*, vol. 34, pp. 835-842, 1988.

[9] ____, "Coding theorem for secret sharing communication-systems with 2 noisy channels," *IEEE Trans. Inform. Theory*, vol. 35, pp. 572-578, 1989.

[10] ____, "A coding theorem for secret sharing communication-systems with 2 Gaussian wiretap channels," *IEEE Trans. Inform. Theory*, vol. 37, pp. 634-638, 1991.

[11] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733-742, 1993.

[12] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography -Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121-1132, 1993.

[13] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inform. Theory*, vol. 46, pp. 344-366, 2000.

[14] ____, "Secrecy capacity for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3047-3061, 2004.

[15] ____, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2437-2452, 2008.

[16] Y. Oohama, "Coding for relay channels with confidential messages," *in Proceedings of the IEEE Information Theory Workshop(ITW)*, Cairns, Australia, pp. 87-89, 2001.

[17] ____, "Capacity Theorems for relay channels with confidential messages," *in Proceedings of the IEEE International Symposium of Information Theory(ISIT)*, Nice, France, pp. 926-930, 2007.

[18] X. He and A. Yener, "On the equivocation region of relay channels with orthogonal components," *in Proceedings of the Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, pp. 883-887, 2007.

[19] ____, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inform. Theory*, vol. 56, pp. 3807-3827, 2010.

[20] Y. Liang and H.V. Poor, "Multiple access channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 54, pp. 976-1002, 2008.

[21] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2493-2507, 2008.

[22] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735-2751, 2008.

[23] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005-4019, 2008.

[24] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 572-584, 1979.

[25] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* Academic Press, New York, 1981.

[26] T. S. Han, *Information-Spectrum Methods in Information Theory.* Springer-Verlag, Berlin, New York, 2002. The Japanese edition was published by Baifukan-publisher, Tokyo, 1998.

[27] Y. Liang and V. V. Veeravalli, "Cooperative relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 53, pp. 900-928, 2007.

[28] Y. Liang and G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 53, pp. 3517-3535, 2007.

[29] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 451-456, 1978.

[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[31] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wire-tap channel," *IEEE Trans. Inform. Theory*, vol. 53, pp. 2933-2945, 2007.